Manual de producto de GFI

GFI EndPointSecurity™

Guía del administrador





Versión del documento: 1.1.1

Última actualización (mes/día/año): 3/20/2014

Tabla de contenido

Lista de figuras

Lista de tablas

1 Introducción

La proliferación de dispositivos de consumo, como iPods, dispositivos USB y teléfonos inteligentes ha aumentado el riesgo de filtraciones de datos y otras actividades malintencionadas deliberadas o no intencionales. Para un empleado, es muy simple copiar grandes cantidades de datos confidenciales en un iPod o un dispositivo USB, o ingresar software ilegal y malintencionado en la red a través de estos dispositivos. GFI EndPointSecurity lo ayuda rápida y fácilmente a combatir estas amenazas críticas sin necesidad de bloquear todos los puertos y alterar sus operaciones diarias.

Temas de este capítulo

1.0.1 Términos y convenciones que se usan en esta guía

Tabla 1: Términos y convenciones que se usan en este manual

Término	Descripción
(icono de información)	Información adicional y referencias esenciales para la operación de GFI EndPointSecurity.
(icono de advertencia)	Notificaciones y precauciones importantes sobre los problemas comunes que pueden surgir.
>	Instrucciones de navegación paso a paso para acceder a una función concreta.
Texto en negrita	Elementos que se seleccionan, como nodos, opciones de menú o botones de comando.
Texto en cursiva	Parámetros y valores que debe reemplazar por el valor aplicable, como rutas de acceso y nombres de archivo personalizados.
`Código`	Indica los valores de texto que se escriben, como comandos y direcciones.

1.1 Amenazas a dispositivos de medios extraíbles

La ventaja clave de los dispositivos de medios extraíbles (o dispositivos portátiles) es el acceso sencillo. En teoría, esto puede ser una gran ventaja para las organizaciones, pero todavía es un hecho conocido que el acceso y la seguridad son extremos opuestos del espectro de seguridad.

Los desarrollos en tecnología de medios extraíbles están incrementando. Las diferentes versiones de dispositivos portátiles, como la memoria flash, han aumentado en lo siguiente:

- Mejor capacidad de almacenamiento
- Rendimiento mejorado
- Instalación rápida y sencilla
- Tamaño físico pequeño de bolsillo.

Como resultado, los usuarios internos pueden realizar lo siguiente de manera deliberada o accidental:

- Llevarse datos confidenciales
- Exponer información confidencial
- Introducir códigos malintencionados (ejemplo: virus, troyanos) que pueden derribar toda la red corporativa
- Transferir material inapropiado u ofensivo al hardware corporativo
- Hacer copias personales de los datos de la compañía y de propiedad intelectual
- Distraerse durante las horas de trabajo.

En un intento por controlar estas amenazas, las organizaciones han comenzado a prohibir el uso de dispositivos portátiles personales en el trabajo. La práctica recomendada indica que nunca debe confiar en el cumplimiento voluntario y la mejor manera de asegurar el control completo de los dispositivos portátiles es poner barreras tecnológicas.

1.2 Acerca de GFI EndPointSecurity

GFI EndPointSecurity es la solución que lo ayuda a mantener la integridad de datos mediante la prevención del acceso no autorizado y la transferencia de contenido hacia y desde los siguientes dispositivos o puertos de conexión:

- Puertos USB (ejemplo: lectores de tarjetas de memoria y flash, pen drives)
- Puertos Firewire (ejemplo: cámaras digitales, lectores de tarjetas Firewire)
- Conexiones de datos inalámbricas (ejemplo: Llaves bluetooth e infrarrojas)
- Unidades de disquete (internas y externas)
- Unidades ópticas (ejemplo: CD, DVD)
- Unidades magnetoópticas (internas y externas)
- Unidades de disco duro USB extraíbles
- Otras unidades como unidades Zip y unidades de cinta (internas y externas).

A través de esta tecnología, GFI EndPointSecurity le permite conceder o rechazar el acceso y asignar privilegios "plenos" o "de solo lectura" a:

- Dispositivos (ejemplo: Unidades de CD/DVD, PDA)
- Usuarios/grupos de usuarios locales o de Active Directory.

Con GFI EndPointSecurity, también puede registrar la actividad de todos los dispositivos o puertos de conexión utilizados en los equipos de destino (incluidas la fecha y hora de uso y las personas que usaron los dispositivos).

1.3 Componentes de GFI EndPointSecurity

Cuando instala GFI EndPointSecurity, se configuran los siguientes componentes:

- Consola de administración de GFI EndPointSecurity
- Agente de GFI EndPointSecurity

1.3.1 Consola de administración de GFI EndPointSecurity

A través de la Consola de administración, puede realizar lo siguiente:

- Crear y administrar directivas de protección y especificar qué categorías de dispositivos y puertos de conectividad se deben controlar
- Implementar directivas de protección y agentes de forma remota en sus equipos de destino equipos de destino. Conceder acceso temporal a los equipos de destino para usar dispositivos específicos
- Ver el estado de protección de dispositivos de cada equipo supervisado
- Llevar a cabo exámenes en los equipos de destino para identificar los dispositivos conectados actual o anteriormente
- Comprobar los registros y analizar qué dispositivos han estado conectados a cada equipo de red
- Realizar un seguimiento de los equipos que tienen un agente implementado y qué agentes requieren actualizaciones.

1.3.2 Agente GFI EndPointSecurity

El agente de GFI EndPointSecurity es un servicio del cliente responsable de la implementación de las directivas de protección en los equipos de destino. Este servicio se instala automáticamente en el equipo de destino de red remoto después de la primera implementación de la directiva de protección relevante a través de la consola de administración de GFI EndPointSecurity. En las siguientes implementaciones de la misma directiva de protección, el agente se actualizará y no se volverá a instalar.

1.4 Funciones clave

GFI EndPointSecurity ofrece las siguientes funciones principales:

Tabla 2: Funciones de GFI EndPointSecurity

Funciones de GFI EndPointSecurity	
Group-based protection control	En GFI EndPointSecurity, puede configurar y colocar equipos en grupos controlados por una directiva de protección. Esto le permite configurar una sola directiva de protección y aplicarla a todos los equipos que son miembros de ese grupo.
Granular access control	GFI EndPointSecurity le permite habilitar o rechazar el acceso a un dispositivo específico, así como asignar (cuando corresponda) privilegios «plenos» o «de solo lectura» a cada dispositivo admitido (por ej., unidades de CD/DVD, PDA) usuario por usuario.
Scheduled deployment	GFI EndPointSecurity le permite programar la implementación de directivas de protección y cambios de configuración relacionados sin necesidad de mantener la consola de administración de GFI EndPointSecurity abierta. La función de implementación también administra las implementaciones fallidas a través de reprogramación automática.

Funciones de GFI EndPointSecurity	
Access control	Aparte de bloquear una variedad de categorías de dispositivos, GFI EndPointSecurity también permite bloquear: » **Por tipo de archivo**: Por ejemplo, permita que el usuario lea archivos *.doc pero bloquee el acceso a todos los archivos *.exe. » **Por puerto físico**: Todos los dispositivos conectados a puertos físicos particulares, por ejemplo, todos los dispositivos conectados a puertos USB. » **Por ID de dispositivo**: Bloquee el acceso a un solo dispositivo en función del ID de hardware único del dispositivo. NOTA En Microsoft Windows 7, se puede usar una función llamada BitLocker To Go para proteger y cifrar los datos cifrados en dispositivos extraíbles. GFI EndPointSecurity realiza comprobaciones en tipos de archivo reales cifrados con Windows 7 BitLocker To Go.
Device whitelist and blacklist	El administrador puede definir una lista de dispositivos específicos que se permiten permanentemente y otros que se excluyen permanentemente.
Power users	El administrador puede especificar usuarios o grupos que siempre tendrán acceso total a los dispositivos que, de lo contrario, están bloqueados por GFI EndPointSecurity.
Temporary access	El administrador puede otorgar acceso temporal a un dispositivo (o grupo de dispositivos) en un equipo en particular. Esta función le permite al administrador generar un código de desbloqueo que el usuario final puede usar para obtener acceso de tiempo limitado a un dispositivo o puerto en particular, incluso cuando el agente de GFI EndPointSecurity no está conectado a la red.
Status dashboard	La interfaz de usuario del panel muestra los estados de los agentes activos e implementados, los servidores de alerta y base de datos, el servicio de GFI EndPointSecurity y datos estadísticos con gráficos. La aplicación principal realiza un seguimiento del estado de los agentes activos al comunicarse con los agentes implementados. Las tareas de mantenimiento se realizan automáticamente una vez que se conecta un agente.
Active Directory deployment through MSI	En la consola de administración de GFI EndPointSecurity, es posible generar archivos MSI que más adelante se pueden implementar con la función Group Policy Object (GPO) dentro de Active Directory u otras opciones de implementación. Un archivo MSI contendrá todos los parámetros de configuración establecidos en una directiva de protección en particular.
Agent management password	Las funciones de administración de agentes (como actualización y desinstalación) están protegidas con una contraseña que el usuario puede configurar. Esto significa que todas las otras instancias de GFI EndPointSecurity no tendrán acceso a las opciones de administración de agentes.
Device discovery	El motor de GFI EndPointSecurity puede utilizarse para examinar y detectar la presencia de dispositivos en la red, incluso en equipos que no tienen ninguna directiva de protección asignada. La información recopilada sobre los dispositivos detectados puede usarse para crear directivas de seguridad y para asignar derechos de acceso para dispositivos específicos.
Logs browser	Una herramienta integrada permite que el administrador examine registros de la actividad del usuario y el uso del dispositivo que detecta GFI EndPointSecurity.
Alerting	GFI EndPointSecurity le permite configurar alertas de correo electrónico, mensajes de red y mensajes SMS que se pueden enviar a determinados destinatarios cuando los dispositivos están conectados o desconectados, cuando se permite o bloquea el acceso al dispositivo y tras eventos generados por el servicio.
Custom messages	Cuando el uso de dispositivos se bloquea para los usuarios, estos reciben mensajes emergentes donde se explican los motivos por los cuales se bloqueó el dispositivo. GFI EndPointSecurity permite la personalización de estos mensajes.
Database maintenance	Para mantener el tamaño del back-end de base de datos, GFI EndPointSecurity puede configurarse para que realice una copia de seguridad o elimine eventos que tengan más de un número personalizado de horas o días de antigüedad.
Device encryption	Para obtener seguridad máxima, GFI EndPointSecurity puede configurarse para que cifre los dispositivos de almacenamiento con cifrado AES 256. El cifrado puede forzarse en equipos específicos al ejecutar agentes en la red.

Funciones de GFI EndPointSecurity	
Data leakage risk assessment	El panel les permite a los usuarios ver posibles riesgos de pérdida de datos en cada extremo. Use las sugerencias proporcionadas y realice las acciones sugeridas para reducir los niveles de riesgo.
Content awareness	La función de reconocimiento de contenido les permite a los usuarios revisar los archivos que ingresan a los extremos a través de dispositivos extraíbles. El contenido se identifica en función de expresiones regulares predefinidas (o personalizadas) y archivos de diccionario. De forma predeterminada, la función busca detalles confidenciales seguros, como contraseñas y números de tarjeta de crédito.

1.5 Cómo funciona GFI EndPointSecurity: Implementación y supervisión

Las operaciones de implementación y supervisión de directivas de protección de GFI EndPointSecurity pueden dividirse en las cuatro etapas lógicas que se describen a continuación:

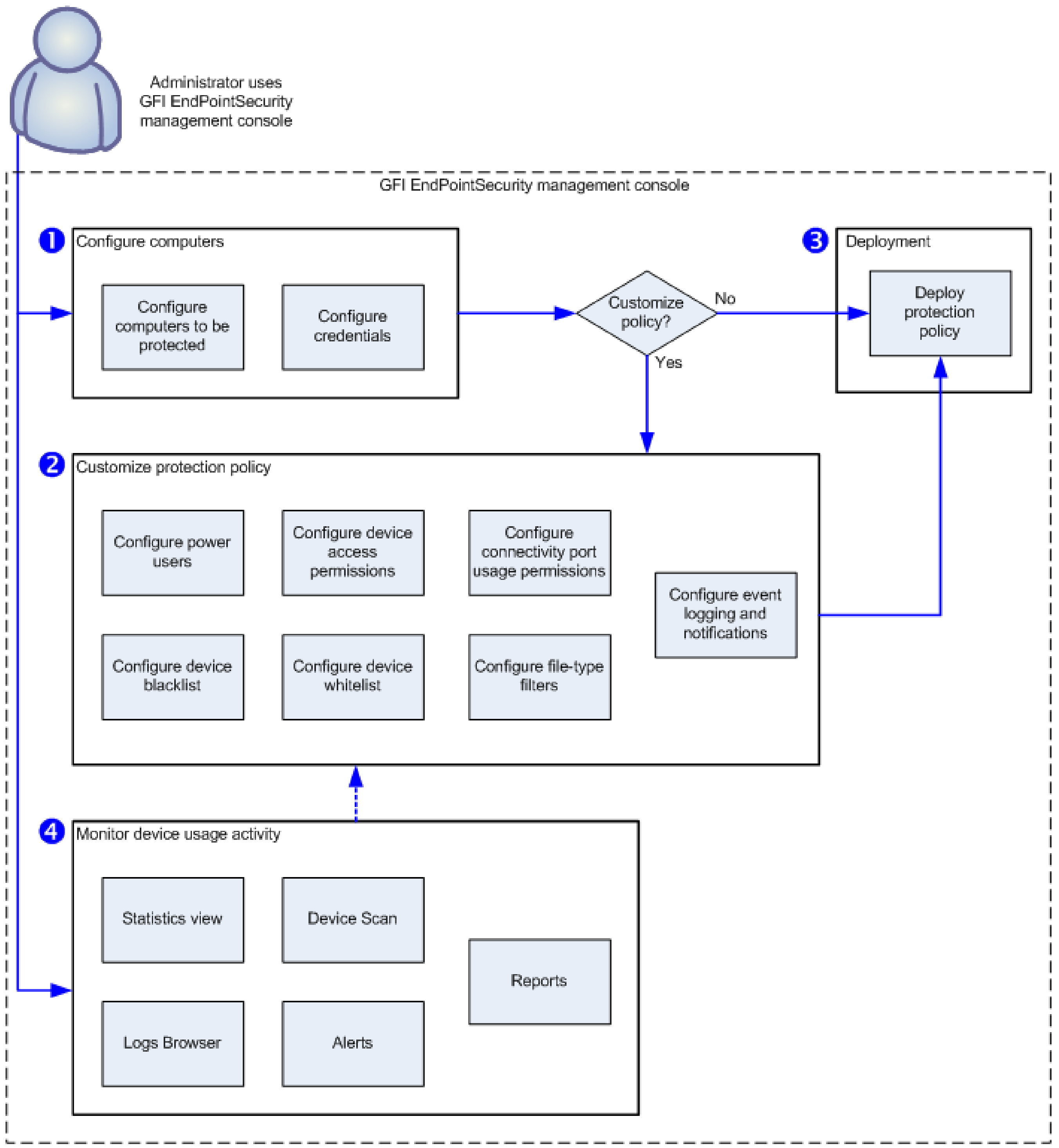


Figura 1: Directiva de protección: Implementación y supervisión

En la siguiente tabla, se describen las etapas detalladas más arriba:

Tabla 3: Implementación y supervisión de la directiva de protección

Etapa	Descripción
Etapa 1: Configurar equipos	El administrador especifica qué directiva de protección se asigna a cada equipo y las credenciales de inicio de sesión que usará GFI EndPointSecurity para acceder a los equipos de destino e implementar los agentes.
Etapa 2: Personalizar la directiva de protección	El administrador puede personalizar una directiva de protección antes o después de implementarla. Las opciones de personalización incluyen la creación de usuarios avanzados, la incorporación de dispositivos de lista negra/lista blanca y los permisos de acceso para dispositivos.

Etapa	Descripción
Etapa 3: Implementar la directiva de protección	El administrador implementa la directiva de protección. En la primera implementación de una directiva de protección, se instala automáticamente un agente de GFI EndPointSecurity en el equipo de destino de red remoto. En las siguientes implementaciones de la misma directiva de protección, el agente se actualizará y no se volverá a instalar.
Etapa 4: Supervisar el acceso a dispositivos	Cuando se hayan implementado los agentes, el administrador puede supervisar todos los intentos de acceso a dispositivos a través de la Consola de administración; recibir alertas y generar informes a través de GFI EndPointSecurity GFI ReportPack.

1.6 Cómo funciona GFI EndPointSecurity: Acceso a dispositivos

Las operaciones de acceso a dispositivos de GFI EndPointSecurity pueden dividirse en tres etapas lógicas:

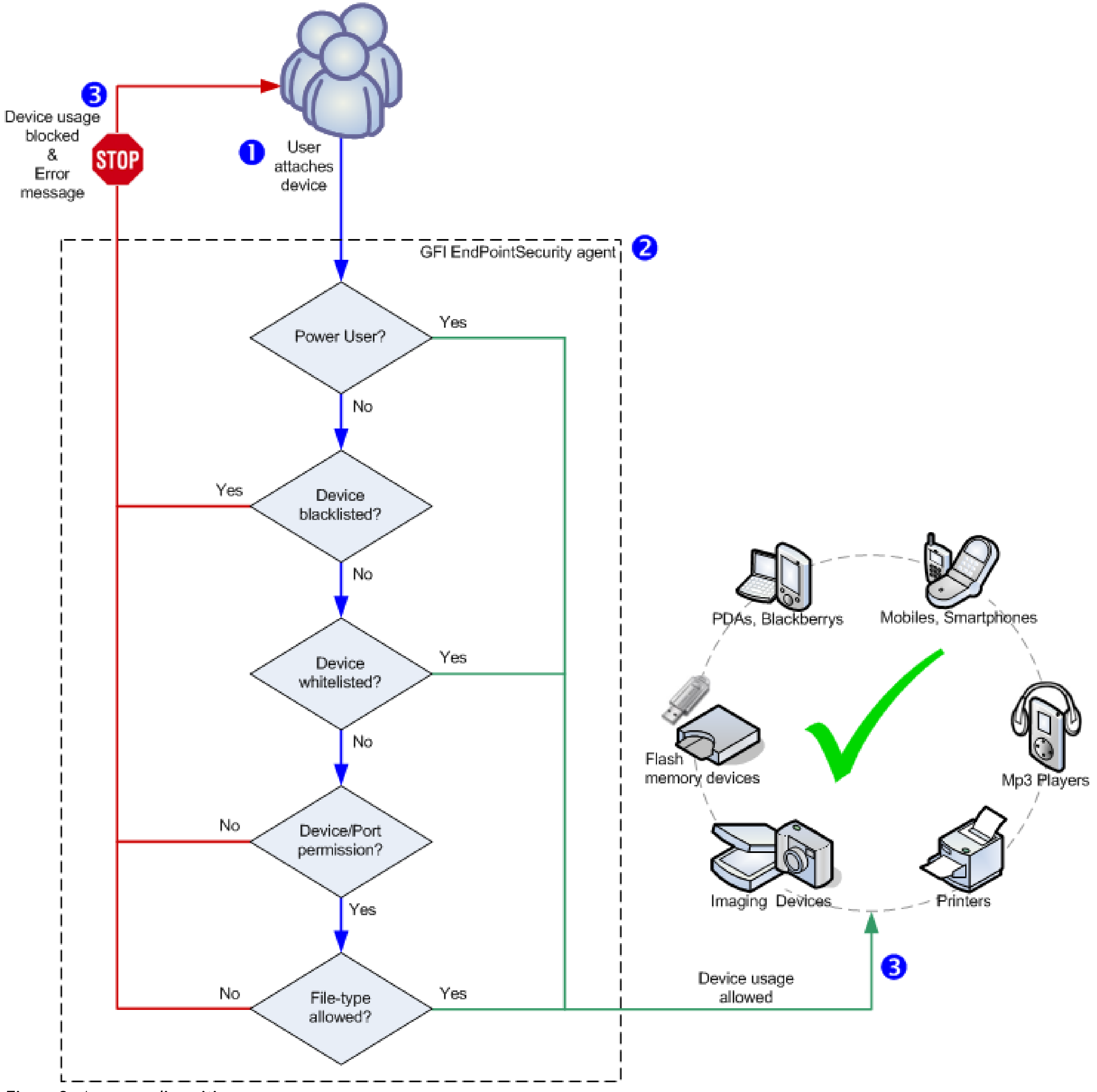


Figura 2: Acceso a dispositivos

En la siguiente tabla, se describen las etapas detalladas más arriba:

Tabla 4: Implementación y supervisión de la directiva de protección

Etapa	Descripción
Etapa 1: Dispositivo conectado a equipo	El usuario conecta un dispositivo a un equipo de destino protegido por GFI EndPointSecurity.
Etapa 2: Aplicación de directiva de protección	El agente de GFI EndPointSecurity instalado en el equipo de destino detecta el dispositivo conectado y pasa por las reglas de la directiva de protección aplicables al equipo/usuario. Esta operación determina si se permite o bloquea el acceso al dispositivo.
Etapa 3: Uso del dispositivo permitido/bloqueado	El usuario recibe un mensaje de error que indica que se ha bloqueado el uso del dispositivo o se le permite el acceso al dispositivo.

1.7 Cómo funciona GFI EndPointSecurity: Acceso temporal

Las operaciones de acceso temporal de GFI EndPointSecurity pueden dividirse en tres etapas lógicas:

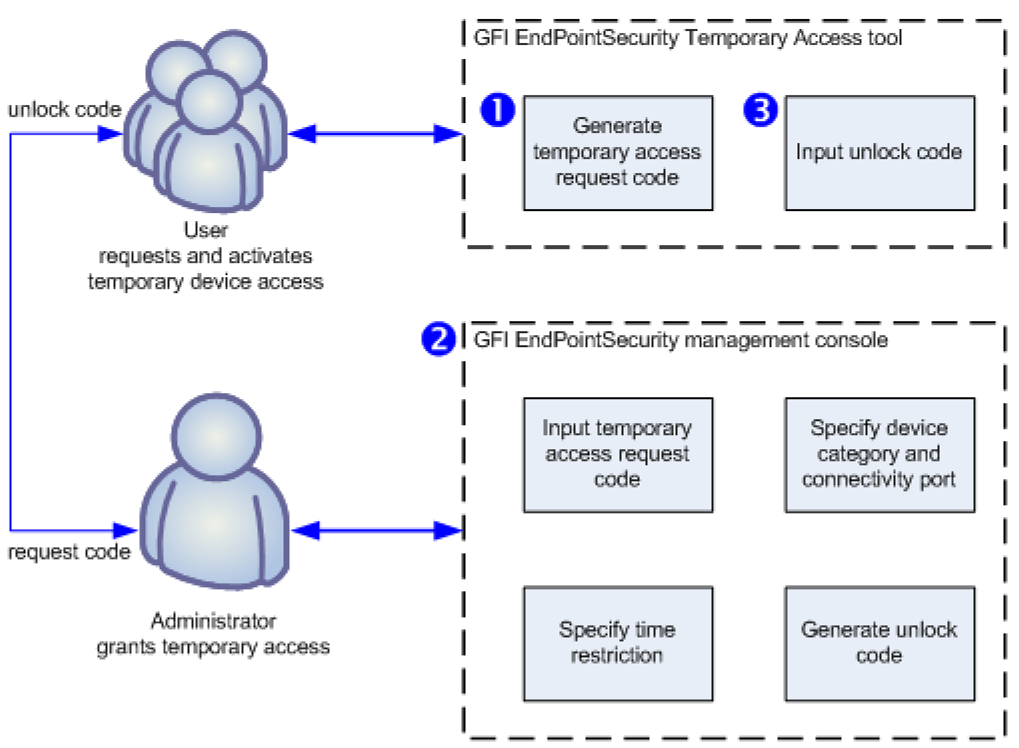


Figura 3: Solicitud/concesión de acceso temporal

En la siguiente tabla, se describen las etapas detalladas más arriba:

Tabla 5: Implementación y supervisión de la directiva de protección

Etapa	Descripción
Etapa 1: El usuario solicita acceso temporal al dispositivo	El usuario ejecuta la herramienta GFI EndPointSecurity Temporary Access desde el equipo desde el que se accederá al dispositivo. La herramienta se usa para generar un código de solicitud, que el usuario le comunica al administrador. El usuario también debe informarle al administrador sobre los tipos de dispositivos y los puertos de conexión a los que debe acceder, y durante cuánto tiempo necesita acceder a estos.
Etapa 2: El administrador otorga acceso temporal	El administrador usa la función Temporary Access dentro de la consola de administración de GFI EndPointSecurity para introducir el código de solicitud y para especificar los dispositivos/puertos y las restricciones de tiempo. Se genera un código de desbloqueo que luego el administrador le comunica al usuario.

Etapa	Descripción
Etapa 3: El usuario activa el acceso temporal al dispositivo	Una vez que el usuario recibe el código de desbloqueo que le envió el administrador, lo introduce en la herramienta GFI EndPointSecurity Temporary Access para activar el acceso temporal y para poder usar los dispositivos/puertos necesarios.

1.8 Categorías de dispositivos admitidas

En GFI EndPointSecurity, los dispositivos se organizan en las siguientes categorías:

Disquetes

CD/DVD

Impresoras

PDA, incluidos:

- Pocket PC
- Teléfonos inteligentes

Adaptadores de red, incluidos:

- Adaptadores Ethernet
- Adaptadores Wi-Fi
- Adaptadores extraíbles (USB, Firewire, PCMCIA)

Módems, incluidos:

- Teléfonos inteligentes
- Teléfonos móviles

Dispositivos de imágenes:

- Cámaras digitales
- Cámaras web
- Escáneres

Dispositivos de interfaz humana (HID):

- Teclados
- Mouse
- Controladores de juegos

Dispositivos de almacenamiento, incluidos:

- Pen drives USB
- Reproductores de medios digitales (por ej., reproductores de MP3/MP4)
- Lectores de tarjetas de memoria y flash

- Dispositivos USB de varias unidades (es decir, dispositivos que no se montan como una unidad única)

Otros dispositivos:

- Llaves/puertos bluetooth
- Llaves/puertos infrarrojos
- Unidades Zip
- Unidades de cinta
- Unidades magnetoópticas (internas y externas).

1.9 Puertos de conectividad admitidos

GFI EndPointSecurity examina los dispositivos que están o han estado conectados en los siguientes puertos:

USB

Secure Digital (SD)

Firewire

Bluetooth

Infrarrojos

PCMCIA

Serie y paralelos

Internos (ejemplo: unidades ópticas conectadas internamente en PCI).

1.10 Exploración de la consola de administración

La consola de administración de GFI EndPointSecurity le proporciona todas las funciones de administración para supervisar y administrar el uso de acceso a dispositivos.

Captura de pantalla 1: Exploración de la interfaz de usuario de GFI EndPointSecurity

La consola de administración de GFI EndPointSecurity consta de las secciones que se describen a continuación:

Sección	Descripción
	Fichas Explore entre las diferentes fichas de la consola de administración de GFI EndPointSecurity. Las fichas disponibles son las siguientes: » **Status**: Supervise el estado de GFI EndPointSecurity y la información estadística sobre el acceso a dispositivos. » **Activity**: Supervise los dispositivos utilizados en la red. » **Configuration**: Acceda y configure las directivas de protección predeterminadas. » **Scanning**: Examine los equipos de destino y detecte dispositivos conectados. » **Reporting**: Descargue o inicie GFI EndPointSecurity GFI ReportPack para generar sus informes. » **General**: Compruebe si hay actualizaciones de GFI EndPointSecurity, así como detalles de licencias y de la versión.
	Subfichas Acceda a más parámetros de configuración o información acerca de la ficha seleccionada de la sección 1.
	Panel izquierdo Acceda a las opciones de configuración proporcionadas en GFI EndPointSecurity. Las opciones de configuración se agrupan en tres secciones, que incluyen **Common Tasks**, **Actions** y **Help**. Están disponibles solo para algunas fichas.
	Panel derecho Configure las opciones de configuración seleccionadas del panel izquierdo. Están disponibles solo para algunas fichas.

2 Instalación de GFI EndPointSecurity

En este capítulo, se proporciona información sobre cómo preparar su entorno de red para implementar GFI EndPointSecurity correctamente.

Temas de este capítulo

2.1 Requisitos del sistema

Requisitos de hardware

En la tabla que aparece a continuación, se muestran los requisitos de hardware para GFI EndPointSecurity y para el agente de GFI EndPointSecurity:

Tabla 6: Requisitos del sistema: Hardware

	GFI EndPointSecurity	GFI EndPointSecurityAgente
Procesador	Mínimo: 2 GHz Recomendado: 2 GHz	Mínimo: 1 GHz Recomendado: 1 GHz
RAM	Mínimo: 512 MB Recomendado: 1 GB	Mínimo: 256 MB Recomendado: 512 MB
Espacio libre	Mínimo: 100 MB Recomendado: 100 MB	Mínimo: 50 MB Recomendado: 50 MB

Sistemas operativos compatibles (x64/x86)

GFI EndPointSecurity y el agente de GFI EndPointSecurity se pueden instalar en un equipo que esté ejecutando cualquiera de los siguientes sistemas operativos:

- Microsoft Windows Server 2012
- Microsoft Windows Small Business Server 2011 (Standard Edition)
- Microsoft Windows Server 2008 R2 (Standard o Enterprise Edition)
- Microsoft Windows Server 2008 (Standard o Enterprise Edition)
- Microsoft Windows Small Business Server 2008 (Standard Edition)
- Microsoft Windows Server 2003 (Standard, Enterprise o Web Edition)
- Microsoft Windows Small Business Server 2003
- Microsoft Windows 8 (Professional o Enterprise)
- Microsoft Windows 7 (Professional, Enterprise o Ultimate Edition)

- Microsoft Windows Vista (Enterprise, Business o Ultimate Edition)
- Microsoft Windows XP Professional Service Pack 3.

Agente: Requisitos de hardware

- Procesador: Velocidad del procesador de 1 GHz o más
- RAM: 256 MB (mínimo); 512 MB (recomendado)
- Disco duro: 50 MB de espacio disponible

Agente: Requisitos de software

- Procesador: Velocidad del procesador de 1 GHz o más
- RAM: 256 MB (mínimo); 512 MB (recomendado)
- Disco duro: 50 MB de espacio disponible

Otros componentes de software

GFI EndPointSecurity requiere los siguientes componentes de software para una implementación completamente funcional:

- Microsoft Internet Explorer 5.5 o superior
- Microsoft .NET Framework 2.0 o superior
- Microsoft SQL Server 2000, 2005 o 2008 como base de datos back-end



Nota

Se requiere un back-end de base de datos para almacenar los datos de acceso a dispositivos y para los informes. GFI EndPointSecurity ofrece la opción de usar una instancia de Microsoft SQL Server disponible o descargar e instalar automáticamente Microsoft SQL Server 2005 Express en el mismo equipo donde está instalada la consola de administración de GFI EndPointSecurity.

Puertos de cortafuegos

Los agentes de GFI EndPointSecurity requieren el **puerto TCP 1116** (predeterminado) para notificarle sus estados a GFI EndPointSecurity y para enviar eventos de acceso a dispositivos. Sin este puerto abierto, el administrador debe supervisar los eventos de cada equipo de destino manual o automáticamente a través de GFI EventsManager. Para obtener más información, consulte http://www.gfi.com/eventsmanager.

2.2 Actualización de GFI EndPointSecurity

Actualización de GFI EndPointSecurity 3 o versiones posteriores

Si tiene GFI LanGuard Portable Storage Control o una versión anterior de GFI EndPointSecurity, es posible actualizar a la versión más reciente de GFI EndPointSecurity. La actualización de GFI EndPointSecurity 3 o versiones posteriores a GFI EndPointSecurity 2013 es sencilla. El proceso de actualización es parte del proceso de instalación de GFI EndPointSecurity 2013, e incluye lo siguiente:

- Desinstalación de GFI EndPointSecurity 3 o versiones posteriores
- Importación de los parámetros de configuración de GFI EndPointSecurity 3.

Al instalar GFI EndPointSecurity, se le pide que confirme si desea importar parámetros de configuración de la versión anterior. Haga clic en **Yes** para importar parámetros de configuración. A continuación, se le pide que especifique cuáles de los siguientes parámetros de configuración desea importar:

- Directivas de protección:
  - Equipo
  - Configuración de seguridad
- Opciones:
  - Opciones de inicio de sesión
  - Opciones de base de datos.

Actualización de GFI LanGuard Portable Storage Control

Si el equipo en el que está instalando GFI EndPointSecurity está protegido con un agente de GFI LanGuardPortable Storage Control, primero debe desinstalar el agente. Para ello:

1. Abra la consola de configuración de GFI LanGuard Portable Storage Control.
2. Elimine el agente del equipo donde se instalará GFI EndPointSecurity.



Nota

Este proceso debe realizarse únicamente para el equipo donde se instalará GFI EndPointSecurity.

3. Cierre la aplicación de la consola de configuración de GFI LanGuard Portable Storage Control y continúe con la instalación de GFI EndPointSecurity.
4. Al instalar GFI EndPointSecurity, se le pide que confirme si desea importar parámetros de configuración de la versión anterior. Haga clic en **Yes** para importar parámetros de configuración.



Nota

Los agentes de GFI LanGuard Portable Storage Control que estaban protegiendo los equipos se agregarán automáticamente a una directiva de protección llamada **LegacyAgents** en GFI EndPointSecurity.

2.3 Instalación de una nueva instancia de GFI EndPointSecurity

Para instalar GFI EndPointSecurity:

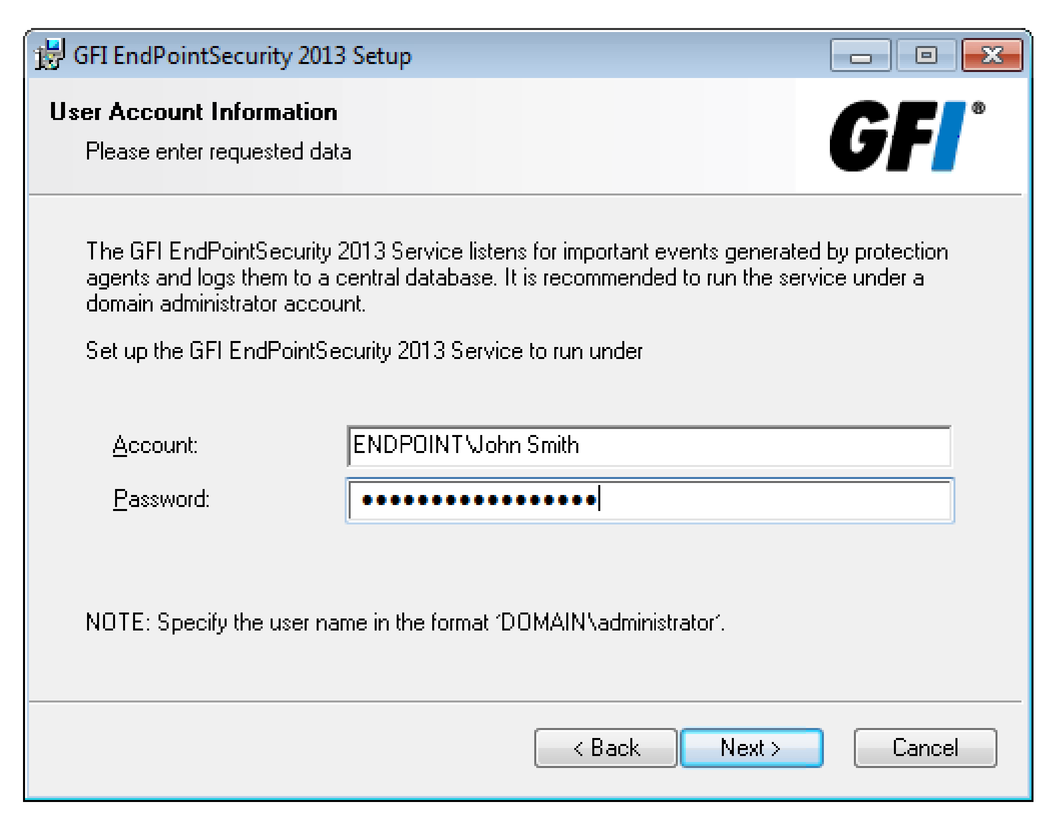
1. Inicie sesión en el equipo donde se instalará GFI EndPointSecurity, con privilegios administrativos.

2. Haga doble clic en el archivo ejecutable GFI EndPointSecurity.

2. Seleccione el idioma que desee instalar y haga clic en **OK**.

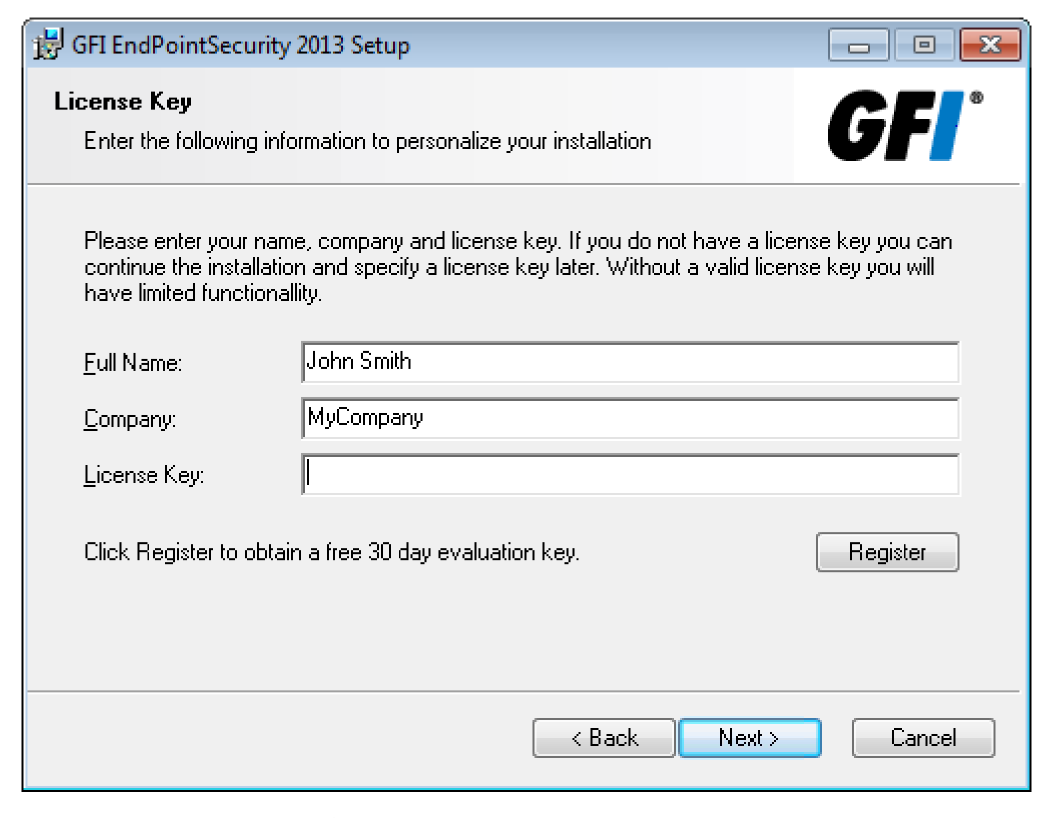
3. Haga clic en **Next** en la pantalla de bienvenida para comenzar la configuración.

4. Lea detenidamente el Acuerdo de licencia para el usuario final. Si está de acuerdo con los términos descritos en el acuerdo, seleccione **I accept the license agreement** y haga clic en **Next**.



Captura de pantalla 2: Instalación de GFI EndPointSecurity: Configuración de la cuenta de administrador de dominio

5. Escriba las credenciales de inicio de sesión de una cuenta con privilegios administrativos y haga clic en **Next** para continuar.



Captura de pantalla 3: Instalación de GFI EndPointSecurity: Detalles de la clave de licencia

6. Complete los campos **Full Name** y **Company**. Si tiene una clave de licencia, actualice los detalles de **License Key** y haga clic en **Next**.



Nota

La clave de licencia se puede completar después de la instalación o del vencimiento del periodo de evaluación de GFI EndPointSecurity. Para obtener más información, consulte Licencias del producto.

7. Escriba o seleccione una ruta de instalación alternativa, o haga clic en **Next** para usar la ruta predeterminada y continuar con la instalación.

8. Haga clic en **Back** para volver a introducir la información de instalación o haga clic en **Next** y espere que finalice la instalación.

9. Cuando se complete la instalación, habilite o deshabilite la casilla de verificación Launch GFI EndPointSecurity y haga clic en **Finish** para finalizar la instalación.

2.4 Parámetros de configuración posteriores a la instalación

En el primer inicio de la consola de administración de GFI EndPointSecurity, se abre automáticamente el asistente para inicio rápido. Esto le permite configurar parámetros importantes de GFI EndPointSecurity para el uso inicial.

El asistente para inicio rápido consta de los siguientes pasos y guías para que configure:

- Evaluación de riesgos
- Detección automática
- Usuarios avanzados
- Grupos de usuarios
- Back-end de base de datos.



Nota

El asistente para inicio rápido se puede volver a iniciar desde **File** > **Quick Start Wizard**.

Para usar el asistente para inicio rápido:

1. Haga clic en **Next** en la pantalla de bienvenida del asistente.
2. En **Risk Assessment**, seleccione o anule la selección de **Start a Risk Scan** para habilitar o deshabilitar la función que inicia un examen de la red para determinar el nivel de riesgo.
3. Opcionalmente, haga clic en **Risk scan settings...** y configure los parámetros para las fichas que se describen a continuación:

Tabla 7: Configuración de detección automática

Ficha	Descripción
Scan Area	Seleccione el área de destino en el cual GFI EndPointSecurity examina los equipos en la red. » **Current domain/workgroup**: GFI EndPointSecurity busca equipos nuevos dentro del mismo dominio/grupo de trabajo donde está instalado. » **The following domains/workgroups**: Seleccione esta opción y haga clic en **Add**. Especifique los dominios donde GFI EndPointSecurity buscará equipos nuevos y haga clic en **OK**. » **Entire network except**: Seleccione esta opción y haga clic en **Add**. Especifique el dominio o grupo de trabajo que se debe ejecutar durante la detección automática y haga clic en **OK**. » **IP range**: Seleccione esta opción y haga clic en **Add**. Especifique el rango de direcciones IP que deben incluirse o ejecutarse durante la detección automática y haga clic en **OK**. » **Computer list**: Seleccione esta opción y haga clic en **Add**. Especifique el dominio o grupo de trabajo que se debe incluir o ejecutar durante la detección automática y haga clic en **OK**.
Logon Credentials	Habilite o deshabilite **Logon using credentials below** y especifique un conjunto de credenciales que GFI EndPointSecurity usará para acceder a los equipos que se examinarán.
Scan Device Categories	Seleccione las categorías de dispositivos que GFI EndPointSecurity incluirá en el examen.
Scan ports	Seleccione los puertos de conexión de dispositivos que GFI EndPointSecurity incluirá en el examen.

4. Haga clic en **Apply** y en **OK** para cerrar el cuadro de diálogo Risk Assessment y haga clic en **Next** en el asistente para inicio rápido.

5. En **Auto Discovery**, seleccione o anule la selección de **Enable Auto Discovery** para activar o desactivar la detección automática. Cuando la detección automática está habilitada, GFI EndPointSecurity examina periódicamente su red para detectar equipos nuevos.

6. Seleccione o anule la selección de **Install agents on discovered computers** para habilitar o deshabilitar la implementación automática de agentes de GFI EndPointSecurity en equipos recientemente detectados.

7. Opcionalmente, haga clic en **Auto discovery settings...** y configure los parámetros para las fichas que se describen a continuación:

Tabla 8: Configuración de detección automática

Ficha	Descripción
Auto Discovery	Habilite o deshabilite la detección automática y configure una programación para que GFI EndPointSecurity examine la red para detectar equipos nuevos.
Discovery Area	Seleccione dónde desea que GFI EndPointSecurity busque equipos nuevos. Seleccione una de las siguientes opciones: » **Current domain/workgroup**: GFI EndPointSecurity busca equipos nuevos dentro del mismo dominio/grupo de trabajo donde está instalado. » **The following domains/workgroups**: Seleccione esta opción y haga clic en **Add**. Especifique los dominios donde GFI EndPointSecurity buscará equipos nuevos y haga clic en **OK**. » **Entire network except**: Seleccione esta opción y haga clic en **Add**. Especifique el dominio o grupo de trabajo que se debe ejecutar durante la detección automática y haga clic en **OK**.
Actions	Configure las acciones que realiza GFI EndPointSecurity cuando se detecta un equipo nuevo. Además, seleccione la directiva a la que se aplica esta configuración.

8. Haga clic en **Apply** y en **OK** para cerrar el cuadro de diálogo Auto Discovery y haga clic en **Next** en el asistente para inicio rápido.

9. En **Power Users**, seleccione o anule la selección de **Set GFI EndPointSecurity Power Users** para habilitar o deshabilitar las funciones de usuarios avanzados. Los miembros del grupo de usuarios

avanzados tienen acceso a cualquier dispositivo conectado en efecto mediante esta directiva.

10. Haga clic en **Select Power Users...** y, en el cuadro de diálogo Power Users, haga clic en **Add...** para agregar usuarios a su dominio/grupo de trabajo.
11. Haga clic en **Apply** y en **OK** para cerrar el cuadro de diálogo Power Users y haga clic en **Next** en el asistente para inicio rápido.
12. En **Users Groups**, seleccione o anule la selección de **Configure Users Groups** para crear usuarios del dominio/grupo de trabajo y enlazarlos con parámetros de configuración de categorías de dispositivos y puertos de conectividad seleccionados en el paso siguiente.
13. Haga clic en **Select which Users Groups to create...**. En el cuadro de diálogo Configure Users Groups, seleccione los dispositivos o puertos de conexión para los cuales se crean los usuarios. Para administrar todos los dispositivos y puertos admitidos desde esta directiva, haga clic en **Select All**.
14. Haga clic en **Close** para cerrar **Configure Users Groups** y haga clic en **Next** en el asistente para inicio rápido.
15. Desde Database, seleccione el tipo de base de datos que desee usar como back-end de base de datos. Seleccione entre las opciones que se describen a continuación:

Tabla 9: Opciones de back-end de base de datos

Opción	Descripción
Don't configure the database at this time	Finalice el asistente para inicio rápido y configure el back-end de base de datos más tarde. Para obtener más información, consulte ACM.
Use an already installed SQL Server instance	Use una instancia de Microsoft SQL Server que ya esté instalada en el mismo equipo en el que está instalando GFI EndPointSecurity o en otro equipo de la red.
Install a local instance of SQL Express Edition	Seleccione esta opción para descargar e instalar una instancia de Microsoft SQL Server Express en el mismo equipo en el que está instalando GFI EndPointSecurity. Se requiere una conexión a Internet.

16. Opcionalmente, haga clic en **Advanced database settings...** para especificar la dirección de SQL Server, el nombre de la base de datos, el método de inicio de sesión y las credenciales respectivas. Haga clic en **Apply** y en **OK** para cerrar el cuadro de diálogo Database Backend.
17. Haga clic en **Next** y espere que se aplique la configuración. Haga clic en **Finish** para cerrar el asistente para inicio rápido.

2.5 Exploración de la consola de administración

La consola de administración de GFI EndPointSecurity le proporciona todas las funciones de administración para supervisar y administrar el uso de acceso a dispositivos.

Captura de pantalla 4: Exploración de la interfaz de usuario de GFI EndPointSecurity

La consola de administración de GFI EndPointSecurity consta de las secciones que se describen a continuación:

Sección	Descripción
	Fichas Explore entre las diferentes fichas de la consola de administración de GFI EndPointSecurity. Las fichas disponibles son las siguientes: » **Status**: Supervise el estado de GFI EndPointSecurity y la información estadística sobre el acceso a dispositivos. » **Activity**: Supervise los dispositivos utilizados en la red. » **Configuration**: Acceda y configure las directivas de protección predeterminadas. » **Scanning**: Examine los equipos de destino y detecte dispositivos conectados. » **Reporting**: Descargue o inicie GFI EndPointSecurity GFI ReportPack para generar sus informes. » **General**: Compruebe si hay actualizaciones de GFI EndPointSecurity, así como detalles de licencias y de la versión.
	Subfichas Acceda a más parámetros de configuración o información acerca de la ficha seleccionada de la sección 1.
	Panel izquierdo Acceda a las opciones de configuración proporcionadas en GFI EndPointSecurity. Las opciones de configuración se agrupan en tres secciones, que incluyen **Common Tasks**, **Actions** y **Help**. Están disponibles solo para algunas fichas.
	Panel derecho Configure las opciones de configuración seleccionadas del panel izquierdo. Están disponibles solo para algunas fichas.

2.6 Prueba de la instalación

Una vez que GFI EndPointSecurity esté instalado y se haya completado el asistente para inicio rápido, pruebe su instalación para asegurarse de que GFI EndPointSecurity funcione correctamente. Siga las instrucciones que se incluyen en esta sección para verificar que la instalación de GFI EndPointSecurity y las operaciones de la directiva de protección predeterminada de envíos funcionen correctamente.

Esta sección contiene la siguiente información:

- Condiciones previas a la prueba
- Caso de prueba
- Volver a la configuración predeterminada

2.6.1 Condiciones previas a la prueba

Las siguientes condiciones previas a la prueba y configuraciones se requieren ÚNICAMENTE para esta prueba:

Configuración del dispositivo

Para la siguiente prueba se requiere:

- Unidad de CD/DVD conectada al equipo local
- Disco de CD/DVD que incluya contenido accesible (preferentemente un disco a cuyo contenido se haya podido acceder antes de la instalación GFI EndPointSecurity).



Nota

Pueden usarse otros dispositivos y medios, como disquetes o pen drives.

Cuentas de usuario

Para esta prueba, asegúrese de tener dos cuentas de usuario disponibles en el mismo equipo donde está instalado GFI EndPointSecurity:

- Una sin privilegios administrativos
- Otra con privilegios administrativos.

Parámetros de configuración

La configuración del asistente para inicio rápido le permite ajustar GFI EndPointSecurity para que se adapte a las necesidades de su compañía, que pueden no coincidir con los parámetros de configuración anteriores a la prueba necesarios. Como resultado, algunos parámetros de configuración de GFI EndPointSecurity deben establecerse como se indica a continuación para que la prueba se realice correctamente:

- Asegúrese de que el equipo local esté incluido en la vista **Status > Agents**. Si el equipo local no está incluido, inclúyalo manualmente en la lista de equipos. Para obtener más información, consulte el manual de administración y configuración de GFI EndPointSecurity.
- Asegúrese de que la directiva de protección predeterminada de envíos esté implementada y actualizada en el equipo local. Para verificarlo, en la vista **Status > Agents** compruebe que:
  - la directiva de protección esté ajustada en control general
  - la implementación esté actualizada
  - el equipo local esté conectado.



Nota

Si la implementación del agente en el equipo local no está actualizada, implemente el agente manualmente. Para obtener más información, consulte el manual de administración y configuración de GFI.

- Asegúrese de que la cuenta de usuario sin privilegios administrativos no esté configurada como usuario avanzado en la directiva de protección de control general (directiva de protección predeterminada de envíos).



Nota

Si la cuenta de usuario está establecida como usuario avanzado, elimínela manualmente del grupo de usuarios avanzados de la directiva de protección de control general (directiva de protección predeterminada de envíos). Para obtener más información, consulte el manual de administración y configuración de GFI EndPointSecurity.

2.6.2 Caso de prueba

Acceso a un disco de CD/DVD

Cuando se cumplan las condiciones previas a la prueba descritas anteriormente, los usuarios no administrativos ya no tendrán acceso a los dispositivos o puertos conectados al equipo local.

Para verificar que el usuario no administrativo no tenga acceso al dispositivo ni a los medios:

1. Inicie sesión en el equipo local como usuario sin privilegios administrativos.
2. Inserte el disco de CD/DVD en la unidad de CD/DVD.

3. En el **Explorador de Windows**, ubique la unidad de CD/DVD y confirme que no puede ver ni abrir el contenido almacenado en el disco de CD/DVD.

Asignación de permisos a usuarios sin privilegios administrativos

Para asignar permisos de acceso a dispositivos de CD/DVD al usuario sin privilegios administrativos:

1. Inicie sesión en el equipo local como usuario con privilegios administrativos.

2. Inicie GFI EndPointSecurity.

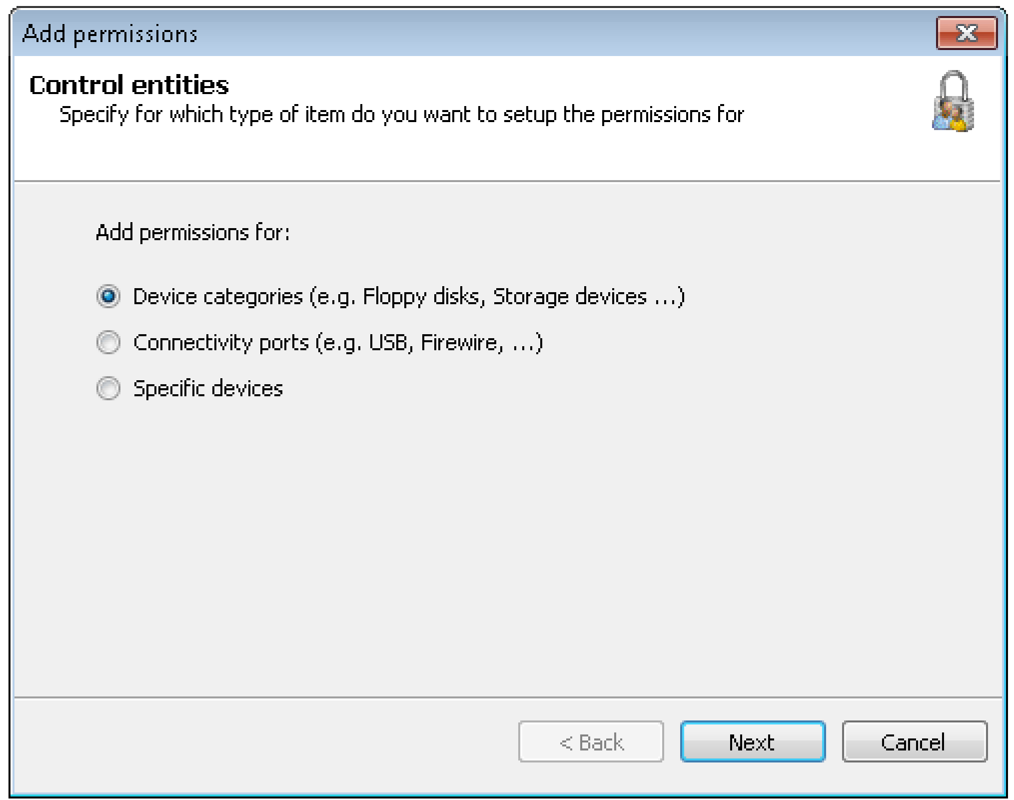
3. Haga clic en la ficha **Configuration**.

4. Haga clic en la subficha **Protection Policies.**

5. En el panel izquierdo, seleccione la directiva de protección **General Control**.

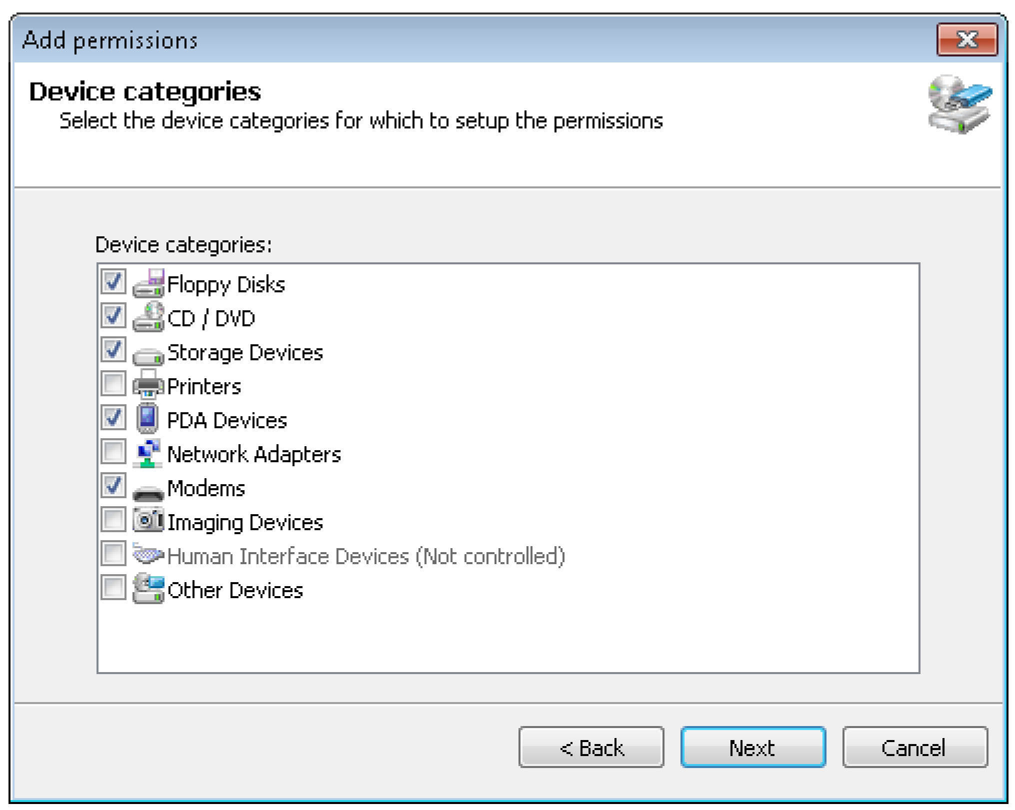
6. Haga clic en el subnodo **Security**.

7. En la sección **Common tasks** del panel izquierdo, haga clic en el hipervínculo **Add permission(s)…**.



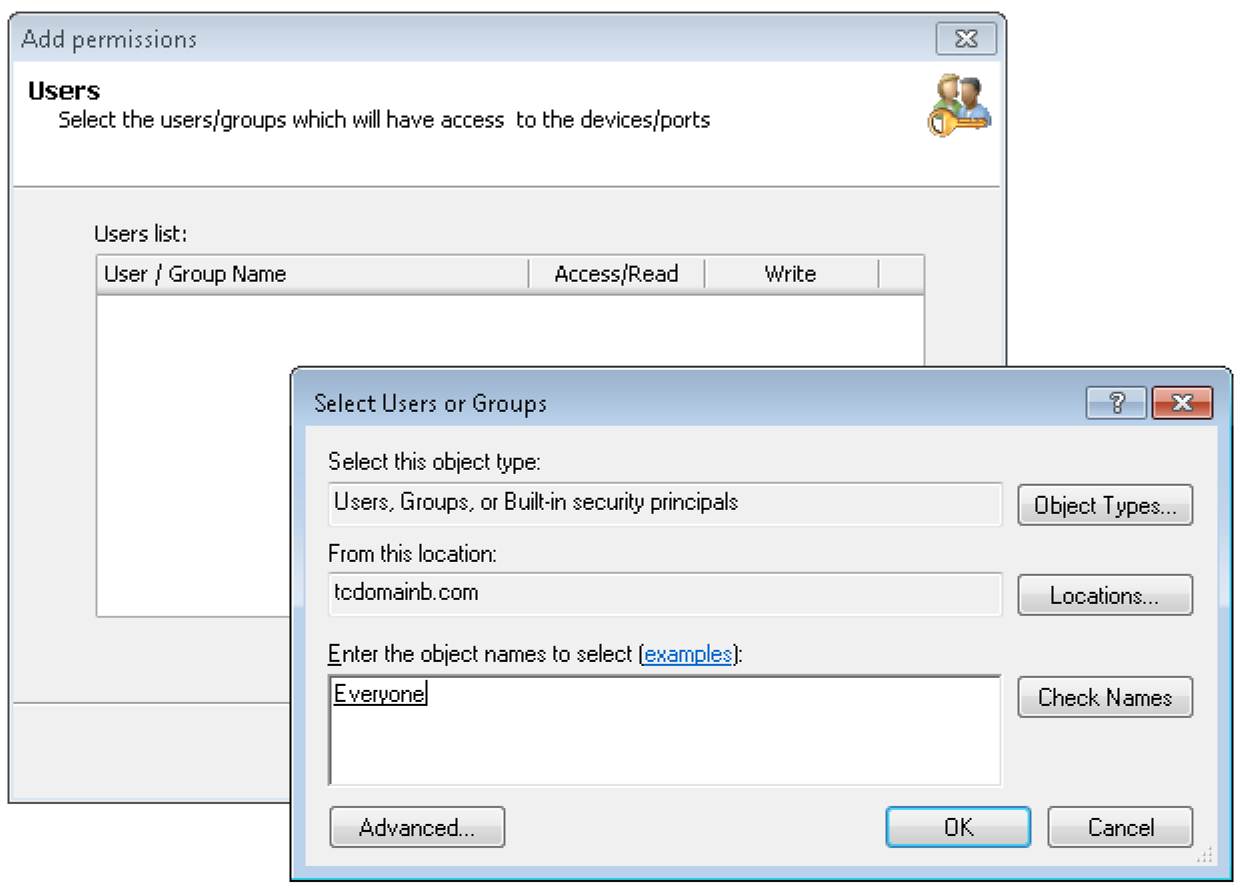
Captura de pantalla 5: Selección de entidades de control

8. En el cuadro de diálogo **Add permissions…**, seleccione la opción **Device categories** y haga clic en **Next** para continuar.



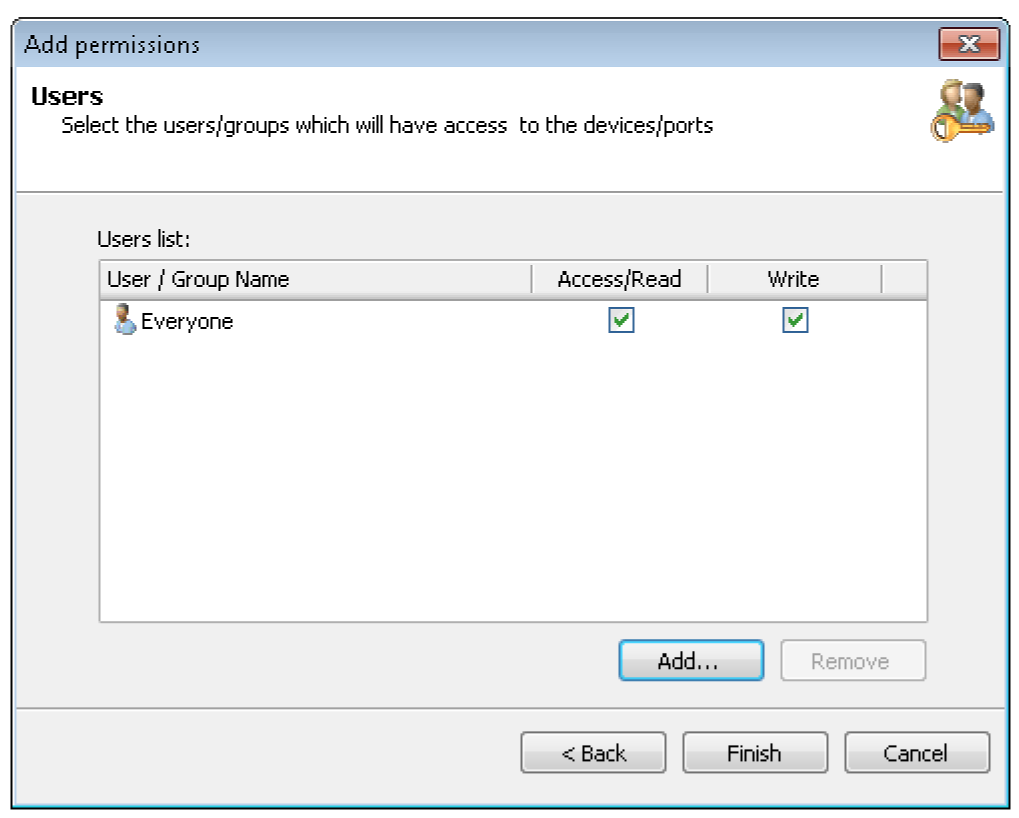
Captura de pantalla 6: Selección de categorías de dispositivos para asignar permisos

9. Habilite la categoría de dispositivo **CD/DVD** y haga clic en **Next**.



Captura de pantalla 7: Incorporación de usuarios o grupos

10. Haga clic en **Add…** y especifique el usuario sin privilegios administrativos que tendrá acceso a la categoría de dispositivo CD/DVD especificada en esta directiva de protección y, a continuación, haga clic en **OK**.



Captura de pantalla 8: Selección de tipos de permisos por usuario o grupo

11. Habilite los permisos **Access/Read** y **Write** y haga clic en **Finish**.

Para implementar actualizaciones de la directiva de protección en el equipo local:

1. En el panel derecho, haga clic en el mensaje de advertencia superior para implementar las actualizaciones de la directiva de protección. La vista debe cambiar automáticamente a **Status > Deployment**.

2. En el área **Deployment History**, confirme que la actualización en el equipo local haya finalizado correctamente.

Nuevo acceso a un disco de CD/DVD

Una vez que se asignen permisos de usuario, el usuario especificado sin privilegios administrativos ahora debe poder acceder a los discos de CD/DVD a través de unidades de CD/DVD conectadas al equipo local.

Para verificar que el usuario no administrativo ahora pueda acceder al dispositivo y a los medios:

1. Inicie sesión en el equipo local como usuario sin privilegios administrativos.

2. Inserte el mismo disco de CD/DVD en la unidad de CD/DVD.

3. En el **Explorador de Windows**, ubique la unidad de CD/DVD y confirme que ahora puede ver y abrir el contenido almacenado en el disco de CD/DVD.

2.6.3 Volver a la configuración predeterminada

Para volver los parámetros de configuración de GFI EndPointSecurity al escenario anterior a la prueba, realice lo siguiente para el usuario sin privilegios administrativos:

1. Si se creó únicamente para esta prueba y ya no es necesaria, quite la cuenta de usuario del equipo local.

2. Incluya al usuario manualmente en la lista de usuarios avanzados, si se configuró como un usuario avanzado antes de esta prueba. Para obtener más información, consulte el manual de administración y configuración de GFI EndPointSecurity.

3. Elimine los permisos de acceso a dispositivos de CD/DVD para el usuario, si no tenía permisos de acceso a dispositivos de CD/DVD antes de esta prueba. Para obtener más información, consulte el manual de administración y configuración de GFI EndPointSecurity.

3 Obtención de resultados

En este capítulo se proporcionan instrucciones paso a paso para bloquear los dispositivos no autorizados de la red y los extremos seguros con GFI EndPointSecurity. A través de este capítulo, puede obtener resultados de cumplimiento legal positivos, y al mismo tiempo asegurarse de que su red esté protegida con las técnicas y los métodos de detección de vulnerabilidades más actualizados.

Temas de este capítulo

3.1 Prevención de filtraciones de datos e infecciones de malware

La mayoría de los hurtos de datos ocurren internamente por parte de empleados que transfieren manualmente los datos a dispositivos de almacenamiento extraíble. El uso de dispositivos de almacenamiento extraíble no autorizados puede exponer a la red a un mayor riesgo de infecciones de malware. GFI EndPointSecurity le permite controlar de manera integral el acceso a los dispositivos de almacenamiento portátil con un esfuerzo administrativo mínimo. Puede otorgarse acceso temporal a los usuarios finales para un dispositivo en un equipo en particular durante un plazo específico.



1. Implementar agentes en equipos que requieren protección

Los agentes de GFI EndPointSecurity se usan para asegurar equipos en la red. Los agentes se pueden implementar manualmente, cuando se instalan agentes en equipos específicos o automáticamente cuando se instalan agentes en cada extremo nuevo detectado en la red. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Incorporación manual de equipos
- Incorporación automática de equipos
- Configuración de credenciales de inicio de sesión.



2. Crear una directiva de protección para bloquear el almacenamiento extraíble

Los agentes aseguran los equipos en función de la configuración de una directiva de seguridad asignada. Puede crear tantas directivas de seguridad como se requieran, y cada directiva puede contener diferentes configuraciones para distintos niveles de autorización. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Creación de directivas de protección
- Asignación de directivas de protección
- Implementación de directivas de inmediato
- Programación de la implementación de directivas
- Implementación de directivas a través de Active Directory
- Comprobación de la implementación de directivas de protección.

3. Establecer la configuración de las directivas de protección

Configure la directiva de protección para bloquear los dispositivos de almacenamiento extraíble. Esto impide que los usuarios finales usen dispositivos que les permiten transferir datos desde y hacia un equipo. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Configuración de categorías de dispositivos controladas
- Configuración de permisos de acceso para categorías de dispositivos
- Configuración de permisos de acceso para dispositivos específicos
- Configuración de prioridades de permisos
- Visualización de permisos de acceso
- Configuración de una lista negra de dispositivos.



4. Configurar alertas de notificación ante intentos de infracción de la directiva de seguridad

GFI EndPointSecurity puede enviar notificaciones a un solo destinatario o a un grupo de destinatarios cuando un usuario final intenta infringir una directiva de seguridad. Esto le permite tomar las medidas necesarias de inmediato y finalizar el uso no autorizado de dispositivos de almacenamiento extraíble. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Configuración de alertas
- Configuración de opciones de alerta
- Configuración de la cuenta del administrador de alertas
- Configuración de destinatarios de las alertas
- Configuración de grupos de destinatarios de las alertas.



5. Configurar el acceso temporal para lograr un uso legítimo de los dispositivos de almacenamiento extraíbles

Si hay una directiva de protección de bloqueo activa, GFI EndPointSecurity le permite habilitar el acceso temporal a un dispositivo para transferir datos de manera legítima desde y hacia un equipo. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Cómo funciona GFI EndPointSecurity: Acceso temporal
- Configuración de usuarios avanzados
- Configuración de privilegios de acceso temporal
- Configuración de una lista blanca de dispositivos
- Configuración de mensajes de usuarios.

3.2 Automatización de la protección de redes

Después de configurar GFI EndPointSecurity, puede proteger automáticamente los equipos nuevos que se detecten en las redes que estén al alcance. Esto puede lograrse al especificar los dominios o los grupos de trabajo que deben examinarse para encontrar equipos nuevos y, cuando GFI EndPointSecurity detecta uno, instala automáticamente un agente y lo asigna a la directiva predeterminada. Las directivas pueden modificarse desde la ficha Configuration > subficha Computers.



1. Descubrir automáticamente dispositivos en la red

Con GFI EndPointSecurity, puede agregar automáticamente equipos nuevos que estén conectados a la red. Esto le permite examinar un dominio o un grupo de trabajo especificados y agregar los equipos que se detecten. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Ejecución de un examen de dispositivos
- Análisis de los resultados del examen de dispositivos
- Incorporación de los dispositivos detectados a la base de datos.



2. Implementar agentes en dispositivos recientemente detectados

GFI EndPointSecurity puede configurarse para que los agentes se instalen automáticamente en los equipos nuevos que se agregan a la base de datos. Se debe instalar un agente en cada equipo que requiera protección. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Incorporación automática de equipos
- Configuración de opciones avanzadas
- Configuración de credenciales de inicio de sesión.



3. Configurar la directiva de protección que se asignará a los dispositivos recientemente detectados (opcional)

Si no se configura una directiva de protección para la implementación, cree una directiva que pueda asignarse a los agentes nuevos que se instalan en los equipos detectados. La directiva predeterminada debe asignarse a un agente nuevo, pero se puede modificar desde la ficha Configuration > subficha Computers. La directiva rige la configuración de seguridad y el comportamiento del dispositivo. Consulte la sección siguiente para obtener información sobre lo que se muestra a continuación:

- Personalización de directivas de protección
- Configuración de una directiva como predeterminada.



4. Asignar directivas de protección automáticamente

Configure GFI EndPointSecurity para que implemente automáticamente directivas de protección en los agentes nuevos. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Programación de la implementación de directivas
- Implementación de directivas a través de Active Directory
- Comprobación de la implementación de directivas de protección.

5. Supervisar la actividad del dispositivo

GFI EndPointSecurity le permite realizar un seguimiento de las auditorías de los registros de actividad generados por los agentes implementados en los equipos de red (el registro de eventos debe estar habilitado). Las fichas Status y Activity le permiten ver los estados e información estadística sobre los extremos, los agentes y GFI EndPointSecurity. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Configuración del registro de eventos
- Visualización de la actividad de uso de dispositivos
- Visualización de estadísticas de uso de dispositivos.

3.3 Supervisión de la actividad de la red desde una ubicación central

Los agentes generan registros de actividad que se almacenan en una base de datos de SQL Server. GFI EndPointSecurity realiza un seguimiento de las auditorías de estos registros y proporciona la información en un conjunto de vistas del panel de información. Las extensas vistas del panel de información de GFI EndPointSecurity le permiten supervisar la actividad de la red en tiempo real, lo cual le permite al administrador tomar medidas inmediatas cuando se detecta un riesgo de seguridad. Configure GFI EndPointSecurity para que genere y envíe informes periódicamente (diariamente/semanalmente/mensualmente) al personal de TI y administración para obtener una vista completa del análisis de los estados de seguridad de los extremos.



1. Analizar la actividad de toda la red

Las subfichas incluidas en las fichas Status y Activity le permiten supervisar la actividad de la red desde una ubicación central. Estas fichas le proporcionan evaluación de riesgos, estadísticas, estados, registros de actividad e información de implementación a través de gráficos y tablas. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Análisis de detalles de la evaluación de riesgos
- Análisis de estadísticas
- Análisis de información de estado
- Análisis de detalles de la implementación del agente
- Análisis de registros de actividad.



2. Generar informes en función de los registros de actividad generados por agentes en la red

GFI EndPointSecurity contiene una extensa lista de informes que pueden utilizarse como están o incluso modificarse para que se ajusten mejor a sus requisitos de informes. ReportPack contiene tanto informes técnicos para el personal de TI como informes ejecutivos con fines de administración. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Uso de GFI EndPointSecurity ReportPack
- Generación de informes de resumen.



3. Mantener el back-end de base de datos

GFI EndPointSecurity almacena registros de eventos en una base de datos de SQL Server. En una red extensa con mucha actividad, el tamaño de la base de datos puede aumentar exponencialmente y el rendimiento de lectura/escritura entre GFI EndPointSecurity y la base de datos puede degradarse. Se recomienda establecer la configuración de retención de registros para que se eliminen automáticamente los eventos antiguos o no deseados, o incluso para que se cree una base de datos nueva cuando la actual alcance un tamaño específico. Consulte las secciones siguientes para obtener información sobre lo que se muestra a continuación:

- Mantenimiento del back-end de base de datos
- Uso de una instancia de SQL Server existente.

4 Incorporación de equipos de destino

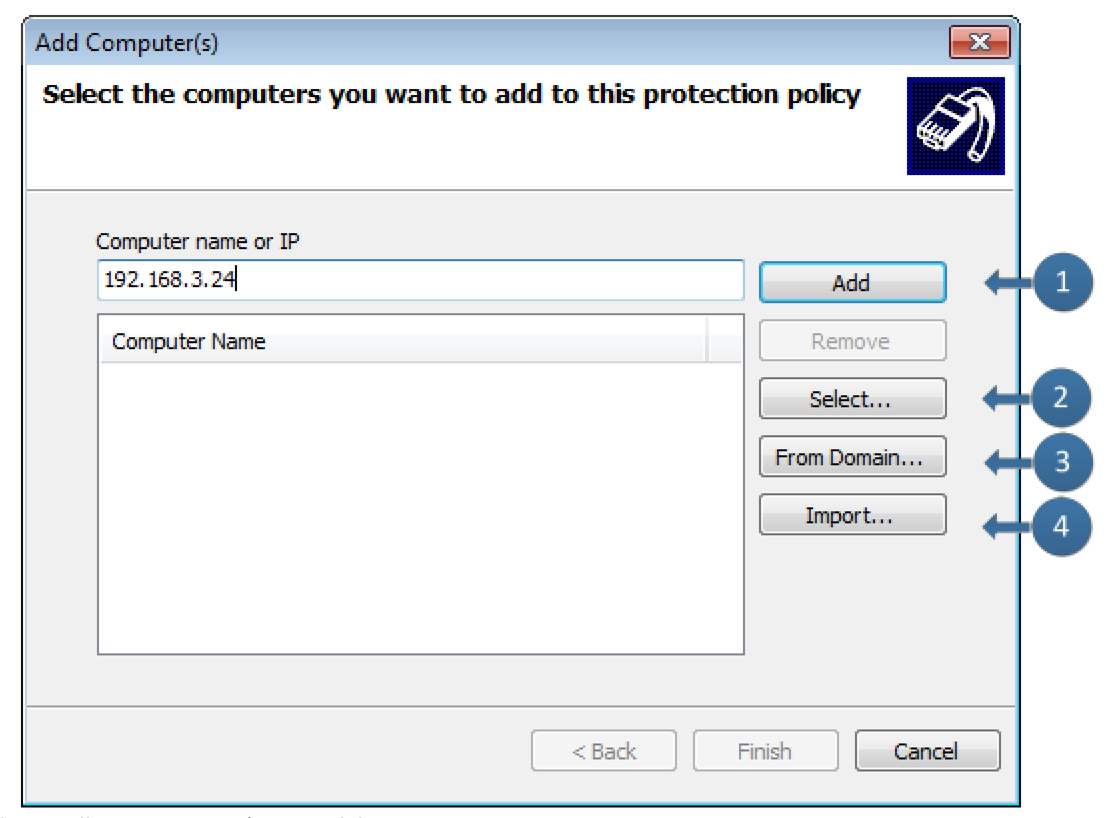
GFI EndPointSecurity le permite especificar los equipos en los que desea implementar agentes y directivas de protección.

Temas de este capítulo

4.1 Incorporación manual de equipos

Para agregar un equipo de destino de forma manual:

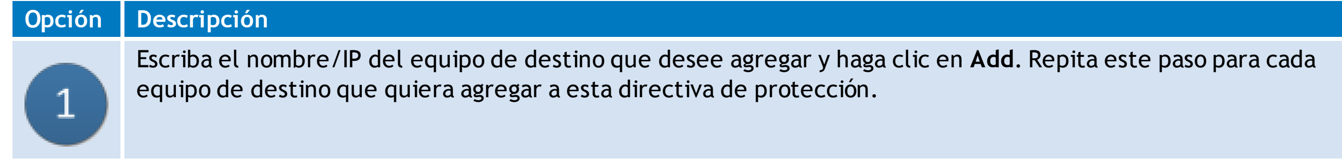
1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Add computer(s)...**.



Captura de pantalla 9: Incorporación manual de equipos

3. En la siguiente tabla se describen las opciones disponibles del cuadro de diálogo **Add Computer (s)**:

Tabla 10: Opciones del cuadro de diálogo Add Computer(s)

Opción	Descripción
 1	Escriba el nombre/IP del equipo de destino que desee agregar y haga clic en **Add**. Repita este paso para cada equipo de destino que quiera agregar a esta directiva de protección.

Opción	Descripción
2	Haga clic en **Select…**. En el cuadro de diálogo **Select Computers**, seleccione el dominio/grupo de trabajo relevante de la lista desplegable y haga clic en **Search**. Habilite los equipos necesarios y haga clic en **OK**.
3	Haga clic en **From Domain…**. Especifique los equipos necesarios desde el dominio/grupo de trabajo donde reside GFI EndPointSecurity.
4	Haga clic en **Import...**. Busque la ubicación del archivo de texto que contiene una lista de los equipos que se importarán. **Nota** Especifique ÚNICAMENTE un nombre de equipo/IP por línea.

4. Haga clic en **Finish**.

4.2 Incorporación automática de equipos

GFI EndPointSecurity le permite buscar y agregar equipos nuevos cuando están conectados a su red a intervalos de tiempo específicos. Esto le permite agregar automáticamente equipos en cuanto se detecten en la red. A través de las funciones de detección automática, puede configurar lo siguiente:

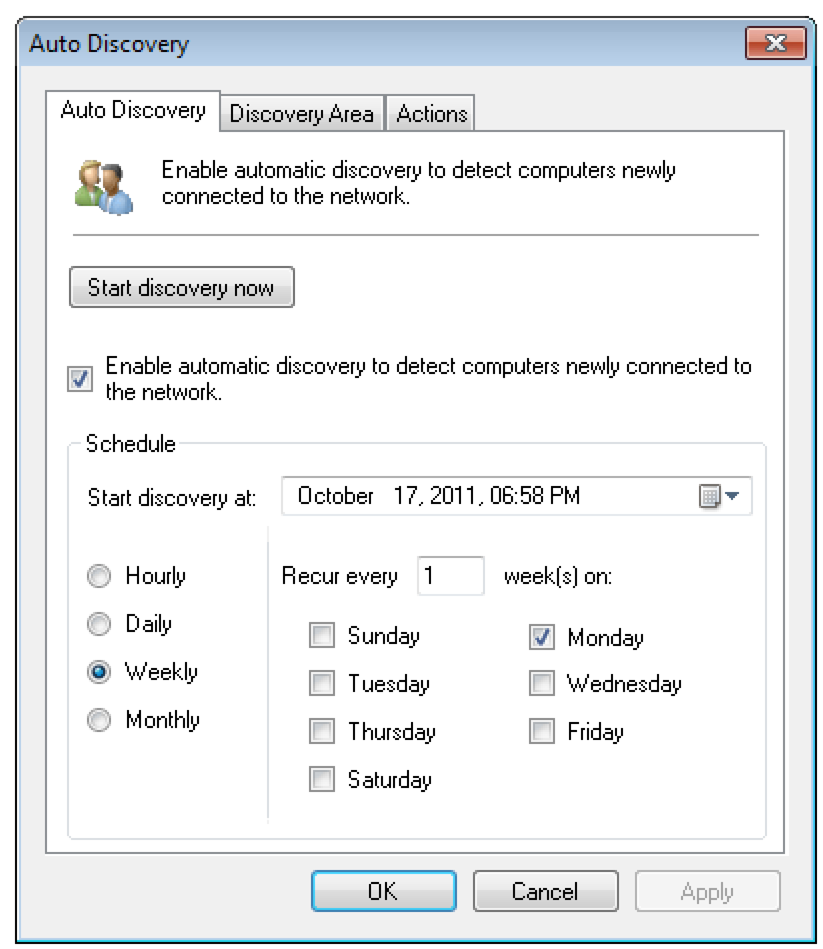
- La frecuencia y la programación de las búsquedas
- El dominio/grupo de trabajo de detección para examinar
- La directiva asignada a los equipos de destino recientemente detectados y las credenciales de inicio de sesión.

De forma predeterminada:

- La configuración de detección automática se establece para examinar el dominio/grupo de trabajo actual (el dominio/grupo de trabajo donde reside GFI EndPointSecurity)
- La configuración del agente de instalación se establece para asignar la directiva de protección de **control general** (directiva de protección predeterminada de envíos) en los equipos recientemente detectados.

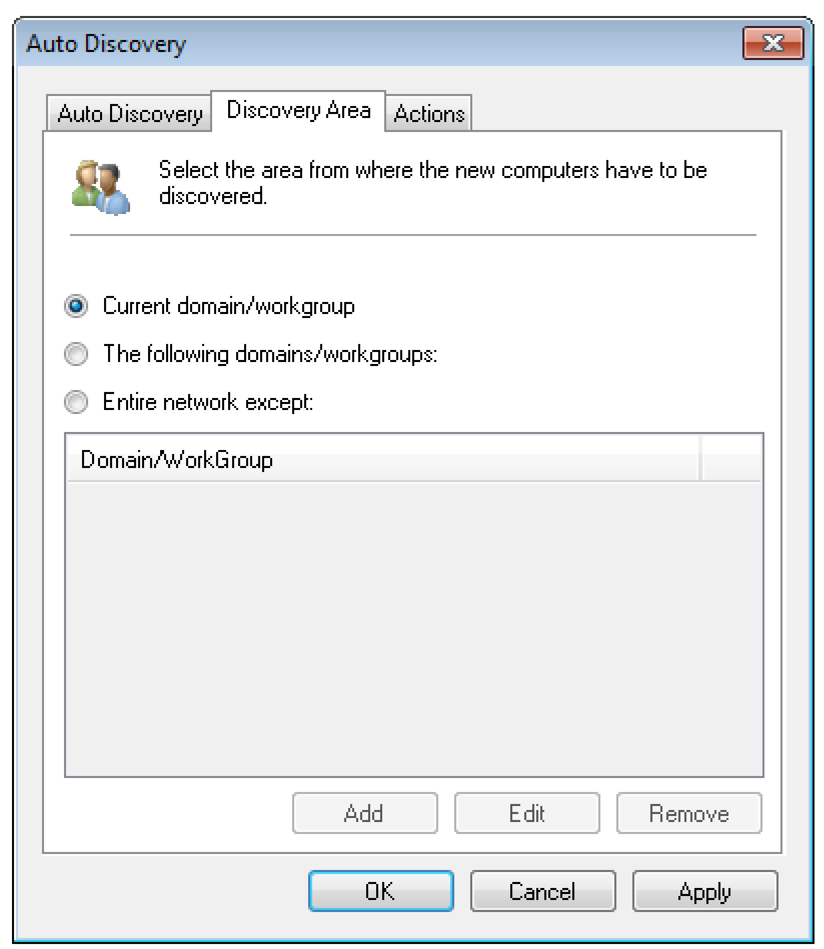
Para ajustar la configuración de detección automática:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Auto discovery settings…**.



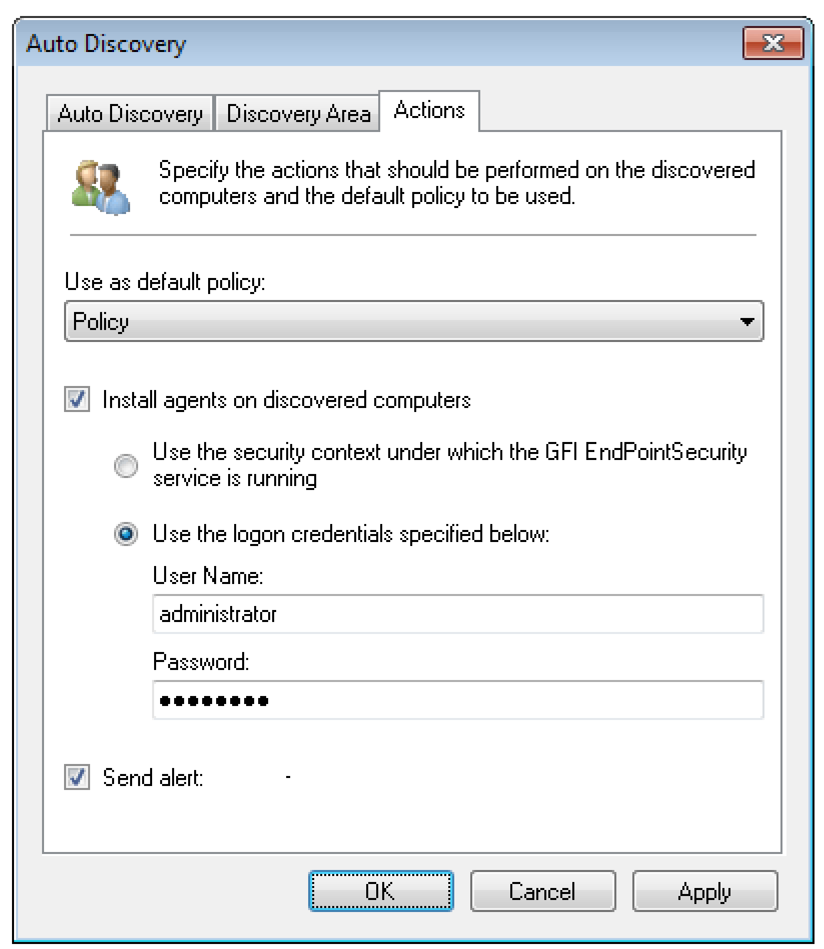
Captura de pantalla 10: Opciones de detección automática: Ficha Auto Discovery

3. Haga clic en **Start discovery now** para ejecutar una detección automática de inmediato.
4. Seleccione o anule la selección de **Enable automatic discovery to detect computers newly connected to the network** para habilitar o deshabilitar la detección automática.
5. En la sección **Schedule**, seleccione la fecha de inicio y establezca la frecuencia de las búsquedas en Hourly, Daily, Weekly o Monthly.



Captura de pantalla 11: Opciones de detección automática: Ficha Discovery Area

6. Haga clic en la ficha **Discovery Area** y seleccione el área para que abarque la detección automática. Para **The following domains/workgroups** y **Entire network except**, haga clic en **Add** y escriba el nombre del dominio/grupo de trabajo.



Captura de pantalla 12: Opciones de detección automática: Ficha Actions

7. Haga clic en la ficha **Actions** y, desde el menú desplegable **Use as default policy**, seleccione la directiva que desee usar para asignar a los equipos recientemente detectados.
8. Seleccione o anule la selección de **Install agents on discovered computers** para habilitar o deshabilitar la implementación automática del agente. Haga clic en **Yes** para confirmar la habilitación de la protección automática.
9. Seleccione el modo de inicio de sesión que GFI EndPointSecurity usa para iniciar sesión en los equipos de destino y para implementar agentes/directivas de protección. De forma predeterminada, GFI EndPointSecurity se configura para usar las credenciales de inicio de sesión de la cuenta del usuario de la sesión actual desde la cual se ejecuta la aplicación de GFI EndPointSecurity.
10. Seleccione o anule la selección de **Send alert** para habilitar o deshabilitar las opciones de alerta. Para obtener más información, consulte Configuración de opciones de alerta (página 131).
11. Haga clic en **Apply** y en **OK**.

4.3 Configuración de credenciales de inicio de sesión

GFI EndPointSecurity requiere que se inicie sesión en los equipos de destino para lo siguiente:

- Implementar agentes y actualizaciones de directivas de protección
- Realizar un seguimiento del estado de protección de todos los equipos de destino.

Esto requiere que GFI EndPointSecurity se ejecute en una cuenta que tenga privilegios administrativos en los equipos de destino de red (ejemplo: una cuenta de administrador de dominio).

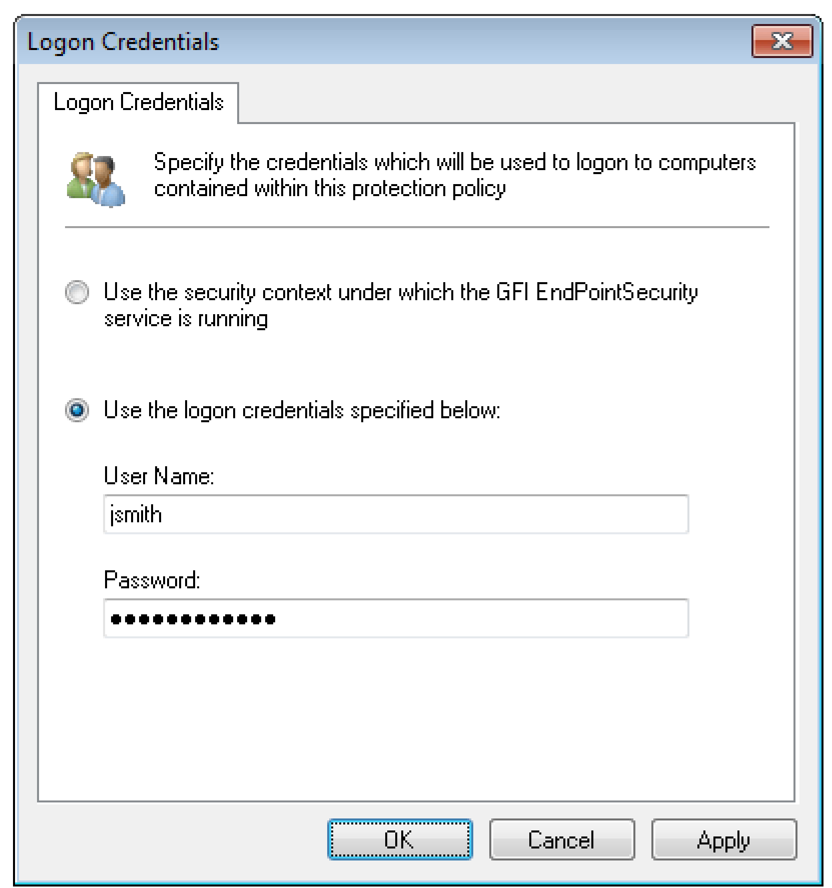
Para especificar credenciales de inicio de sesión para un equipo de destino:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. Haga clic con el botón secundario en un equipo de la lista y haga clic en **Set logon credentials...**.



Nota

Si desea establecer varios equipos para iniciar sesión con las mismas credenciales, resalte los equipos necesarios, haga clic con el botón secundario en uno de ellos y haga clic en **Set logon credentials...**. Como alternativa, haga clic en **Set logon credentials...** desde **Actions**.



Captura de pantalla 13: Opciones del cuadro de diálogo Logon Credentials

3. En la siguiente tabla se describen las opciones de credenciales de inicio de sesión disponibles:

Tabla 11: Opciones de credenciales de inicio de sesión

Opción	Descripción
Use the security context under which GFI EndPointSecurity service is running	Se utilizan las mismas credenciales que están ejecutando GFI EndPointSecurity.
Use the logon credentials specified below	Se especifican credenciales alternativas para usar cuando se inicia sesión en equipos de destino remotos. **Nota** Se especifican credenciales que tengan privilegios administrativos en los destinos del examen.

4. Haga clic en **Apply** y en **OK**.



Nota

De forma predeterminada, GFI EndPointSecurity se configura para usar las credenciales de inicio de sesión de la cuenta del usuario de la sesión actual, que ejecuta GFI EndPointSecurity.

5 Administración de directivas de protección

En este capítulo, se describe cómo implementar directivas de protección creadas recientemente y cómo programarlas. Antes de la implementación, también puede modificar la configuración de su directiva de protección.

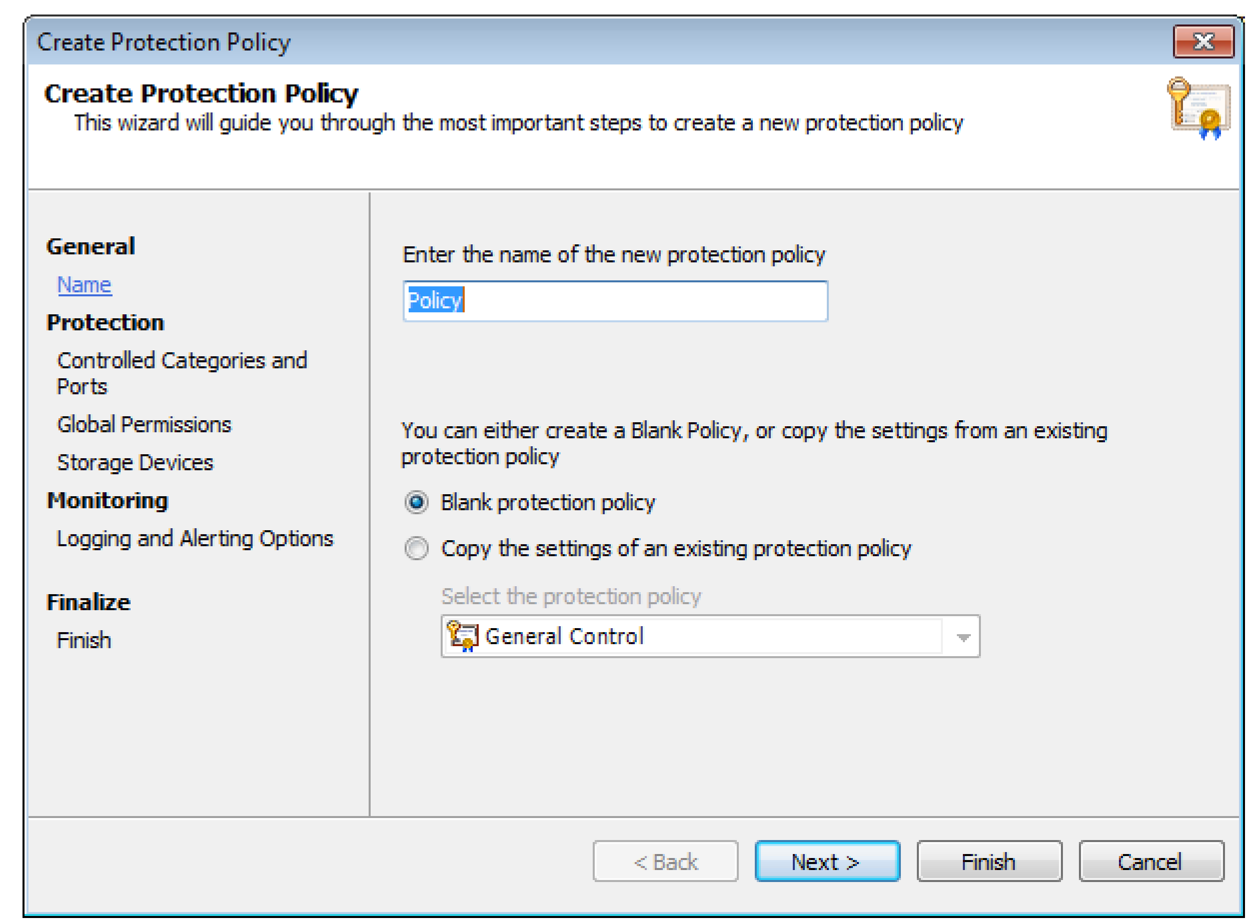
Temas de este capítulo

5.1 Creación de una directiva de protección nueva

GFI EndPointSecurity se ofrece con una directiva de protección predeterminada para que el software funcione después de la instalación. Puede crear otras directivas de protección para que se ajusten a las directivas de seguridad de acceso a dispositivos de su compañía.

Para crear una directiva de protección nueva:

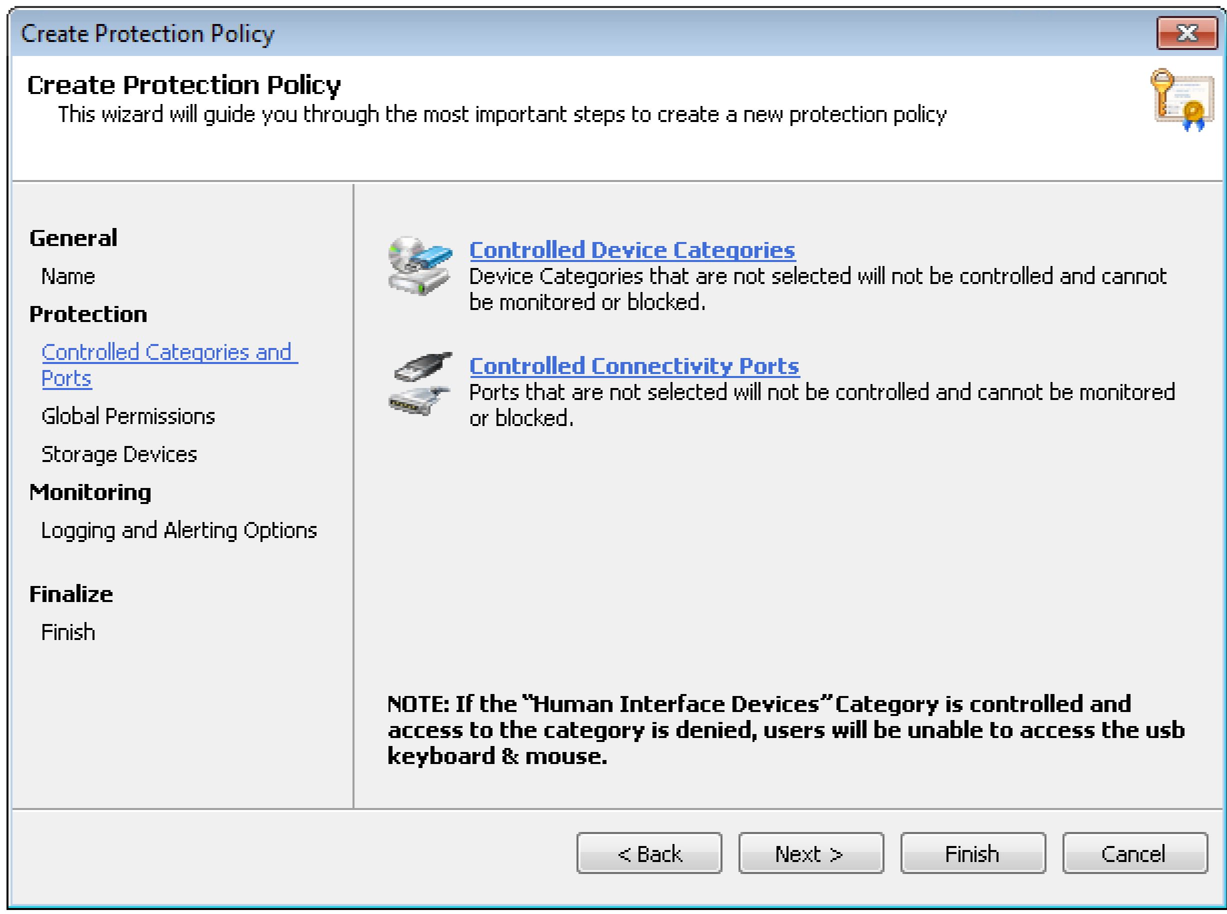
1. Haga clic en la ficha **Configuration** > **Protection Policies**.
2. En **Common tasks**, haga clic en **Create new protection policy...**.



Captura de pantalla 14: Creación de una directiva nueva: Configuración general

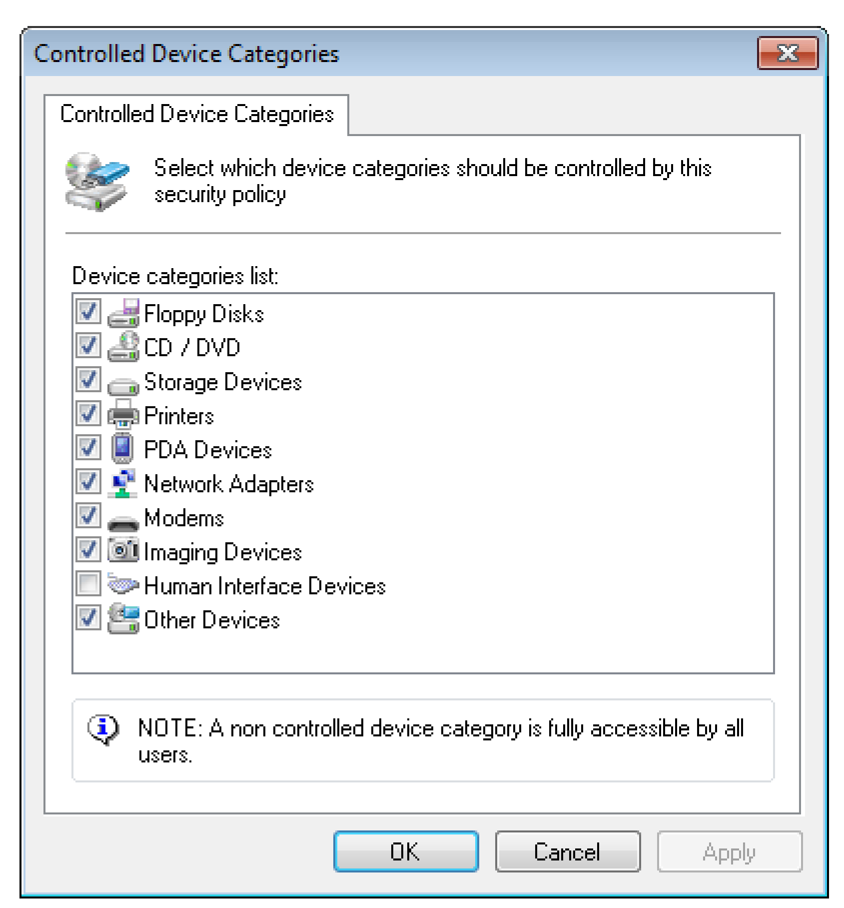
3. Escriba un nombre único para la directiva de protección nueva.

4. Seleccione si desea crear una directiva en blanco o copiar la configuración de una directiva existente. Haga clic en **Next**. En el área de configuración, seleccione la opción de herencia de configuración necesaria:



Captura de pantalla 15: Creación de una directiva nueva: Configuración de categorías y puertos controlados

5. Haga clic en **Controlled Device Categories**.



Captura de pantalla 16: Opciones de categorías de dispositivos controladas

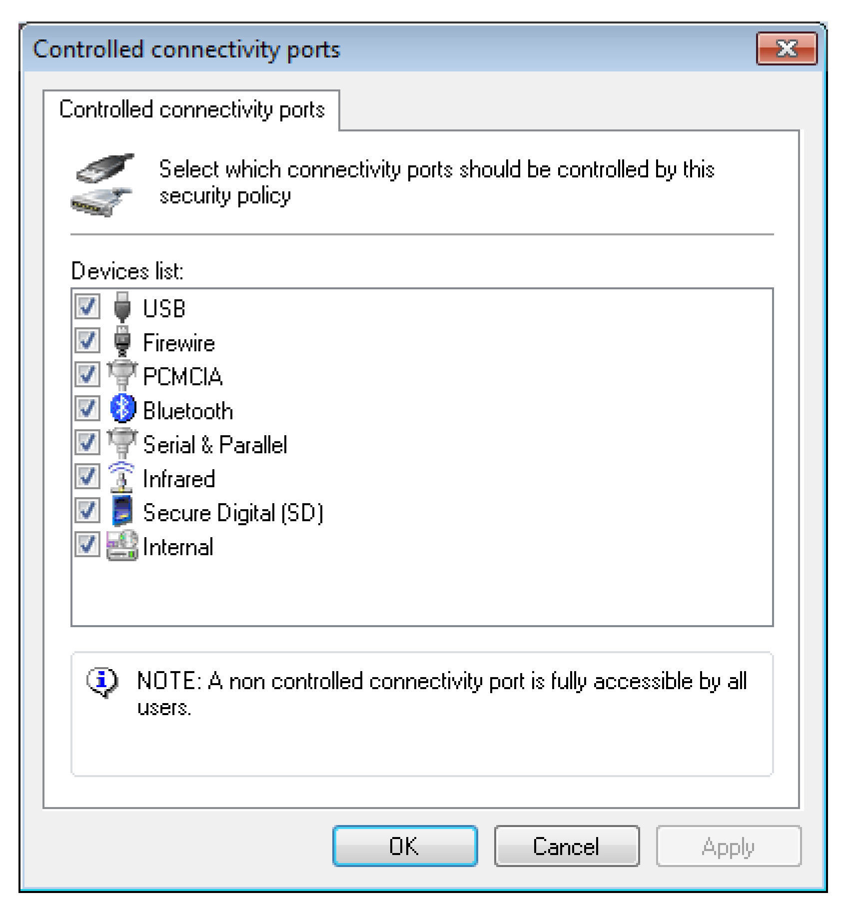
6. En el cuadro de diálogo **Controlled Device Categories**, seleccione las categorías de dispositivos que desee que se controlen con esta nueva directiva. Haga clic en **OK** para cerrar el cuadro de diálogo **Controlled device categories** y regresar al asistente.



Importante

Si la opción Human Interface Devices está habilitada y se rechaza el acceso, los usuarios no podrán usar ratones y teclados USB conectados a los equipos de destino protegidos por esta directiva.

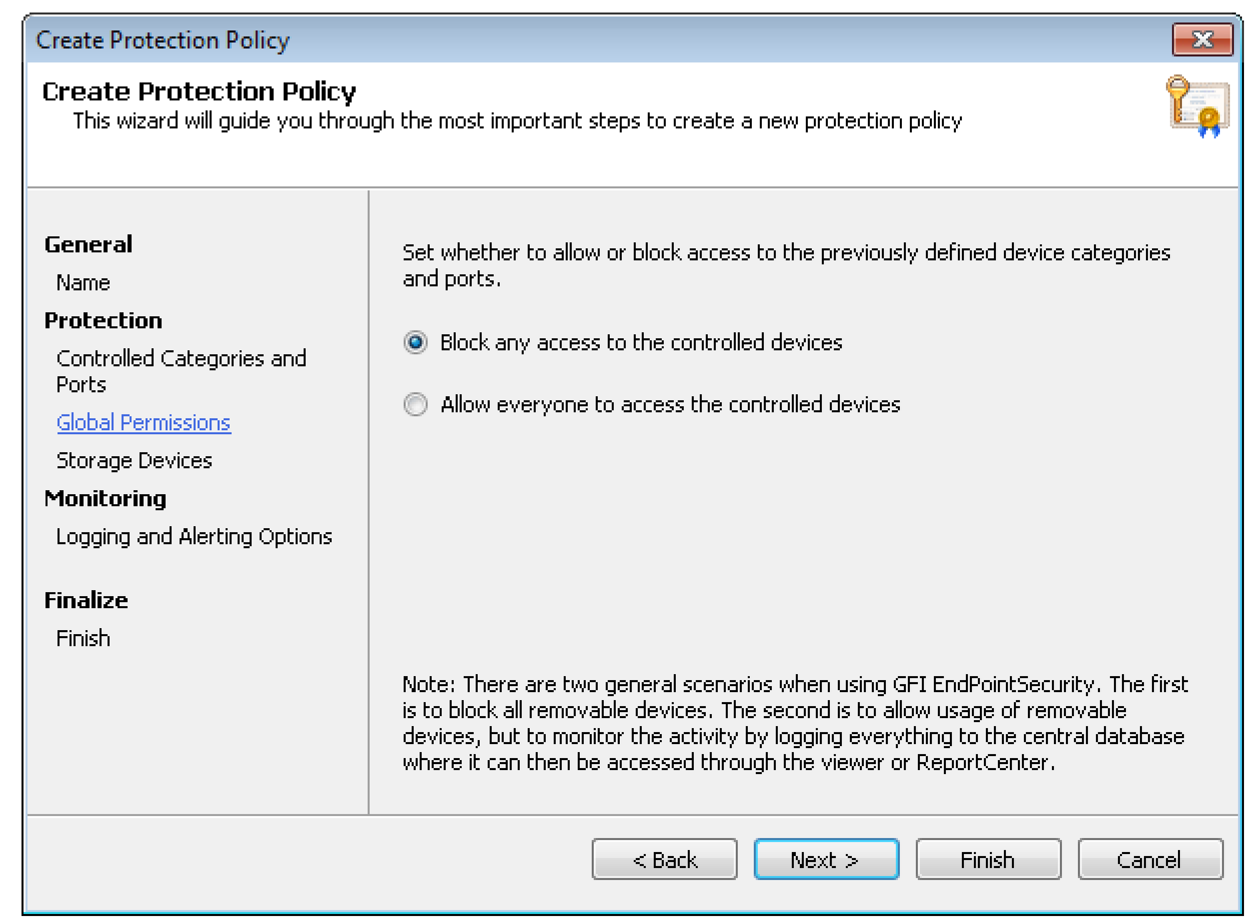
7. Haga clic en **Controlled Connectivity Ports.**



Captura de pantalla 17: Opciones de puertos de conectividad controlados

8. En el cuadro de diálogo **Controlled connectivity ports**, seleccione los puertos de conectividad que desee que se controlen con esta nueva directiva. Haga clic en **OK** para cerrar el cuadro de diálogo **Controlled connectivity ports** y regresar al asistente.

9. Haga clic en **Next**.



Captura de pantalla 18: Creación de una directiva nueva: Configuración de permisos globales

10. En el cuadro de diálogo **Global Permissions**, seleccione los permisos de acceso global necesarios:

- **Block any access to the controlled devices**: para bloquear el acceso a todos los dispositivos/puertos seleccionados.
- **Allow everyone to access the controlled devices**: para permitir el acceso a todos los dispositivos/puertos seleccionados. Si se selecciona esta opción, igualmente se realizará la supervisión de actividad en los equipos de destino abarcados por esta directiva de protección.

11. Haga clic en **Next**.
12. Haga clic en **File-Type Filter** y agregue los tipos de archivo para bloquear o permitir con esta directiva.



Nota

GFI EndPointSecurity le permite restringir el acceso en función de tipos de archivo. También es posible identificar el contenido real de los tipos de archivo más comunes (ejemplo: .DOC o .XLS) y realizar las acciones necesarias correspondientes para el tipo de archivo verdadero. Esto es útil principalmente cuando se manipulan extensiones de archivo de manera malintencionada. Para obtener más información, consulte Configuración de filtros por tipo de archivo (página 83).

13. Haga clic en **OK** para cerrar el cuadro de diálogo **File-Type Filter** y regresar al asistente.
14. Haga clic en **Encryption** y habilite o configure el motor de cifrado que prefiera.



Nota

Además, GFI EndPointSecurity también puede permitir o prohibir que usuarios o grupos de usuarios de Active Directory (AD) accedan a tipos de archivo específicos almacenados en dispositivos cifrados con BitLocker To Go. Estas restricciones se aplican cuando los dispositivos cifrados se conectan a los equipos de destino abarcados por la directiva de protección. Para obtener más información, consulte Configuración de cifrado de seguridad (página 90).

15. Haga clic en **OK** para cerrar el cuadro de diálogo **Encryption** y regresar al asistente.
16. Haga clic en **Next**.

Create Protection Policy

Create Protection Policy
This wizard will guide you through the most important steps to create a new protection policy

General
Name
Protection
Controlled Categories and Ports
Global Permissions
Storage Devices
Monitoring
Logging and Alerting Options
Finalize
Finish

File-Type Filter
Control access to files by file type. Identify the file type from the content for most common file types.

Content Awareness
Control access to files with specific content.

Note: By setting a file type and/or content filter, devices from the Storage Device category will be accessible for everyone and the control will be done based on the file type and/or the content filter.

File Options
Set general options to be used when checking accessed files.

Encryption
Storage Devices can be encrypted to protect contained data. A protection policy can specify how an encrypted device will be controlled.

< Back | Next > | Finish | Cancel

17. En **Storage Devices**, seleccione las opciones necesarias que desee controlar desde las fichas que se describen a continuación:

Tabla 12: Configuración de detección automática

Ficha	Descripción
File-Type Filter	GFI EndPointSecurity le permite especificar restricciones por tipo de archivo en los archivos, como .DOC o .XLS, que se copian en los archivos permitidos y desde ellos. Puede aplicar estas restricciones a usuarios o grupos de usuarios de Active Directory (AD).

Ficha	Descripción
Content Awareness	GFI EndPointSecurity le permite especificar las restricciones de contenido de los archivos para una directiva de protección en particular. La función de reconocimiento de contenido revisa los archivos y traduce los extremos a través de dispositivos extraíbles e identifica el contenido en función de expresiones regulares preconfiguradas y personalizadas y archivos de diccionario. De forma predeterminada, el módulo busca detalles confidenciales seguros como números de seguridad social y números de cuenta primarios, así como información relacionada con empresas y compañías como nombres de enfermedades, fármacos, productos químicos peligrosos y lenguaje trivial o términos étnicos/racistas. » Puede configurar comprobaciones de contenido como una directiva global de manera similar al módulo de comprobación de archivos.
File Options	GFI EndPointSecurity le permite especificar las opciones necesarias para bloquear o permitir archivos en función del tamaño. GFI EndPointSecurity también le permite ignorar archivos de gran tamaño al comprobar el tipo de archivo, el contenido y los archivos almacenados.
Encryption	GFI EndPointSecurity le permite configurar los parámetros que se adaptan específicamente a los dispositivos cifrados. También le permite cifrar dispositivos que todavía no están asegurados.



Nota

Para obtener más información, consulte Personalización de directivas de protección (página 59).

18. Configure las opciones de alerta y de registro de esta directiva y haga clic en **Next**.



Nota

Para obtener más información, consulte Configuración del registro de eventos y Configuración de alertas.

19. Para obtener información acerca de su directiva, revise la página de resumen y haga clic en **Finish**.

5.2 Asignación de una directiva de protección

El siguiente paso es vincular el conjunto de permisos de puertos de conectividad y acceso a dispositivos relevante a cada equipo de destino. Puede hacerlo al asignar directivas de protección a equipos de destino.



Nota

Los equipos de destino solo pueden tener una directiva de protección asignada a la vez.

Para asignar una directiva de protección a un equipo de destino:

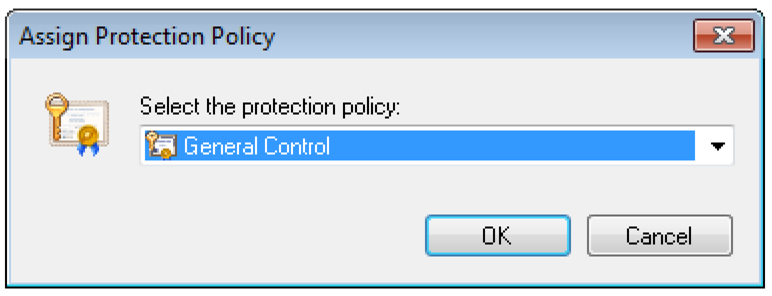
1. En la consola de administración de GFI EndPointSecurity, seleccione **Configuration**.
2. Haga clic en **Computers**.
3. Resalte los equipos de destino necesarios.



Nota

Si desea asignar la misma directiva a más de un equipo de destino, seleccione todos los equipos de destino necesarios y, a continuación, especifique la directiva de protección para el conjunto seleccionado.

4. En la sección **Actions** del panel izquierdo, haga clic en **Assign Protection Policy**.



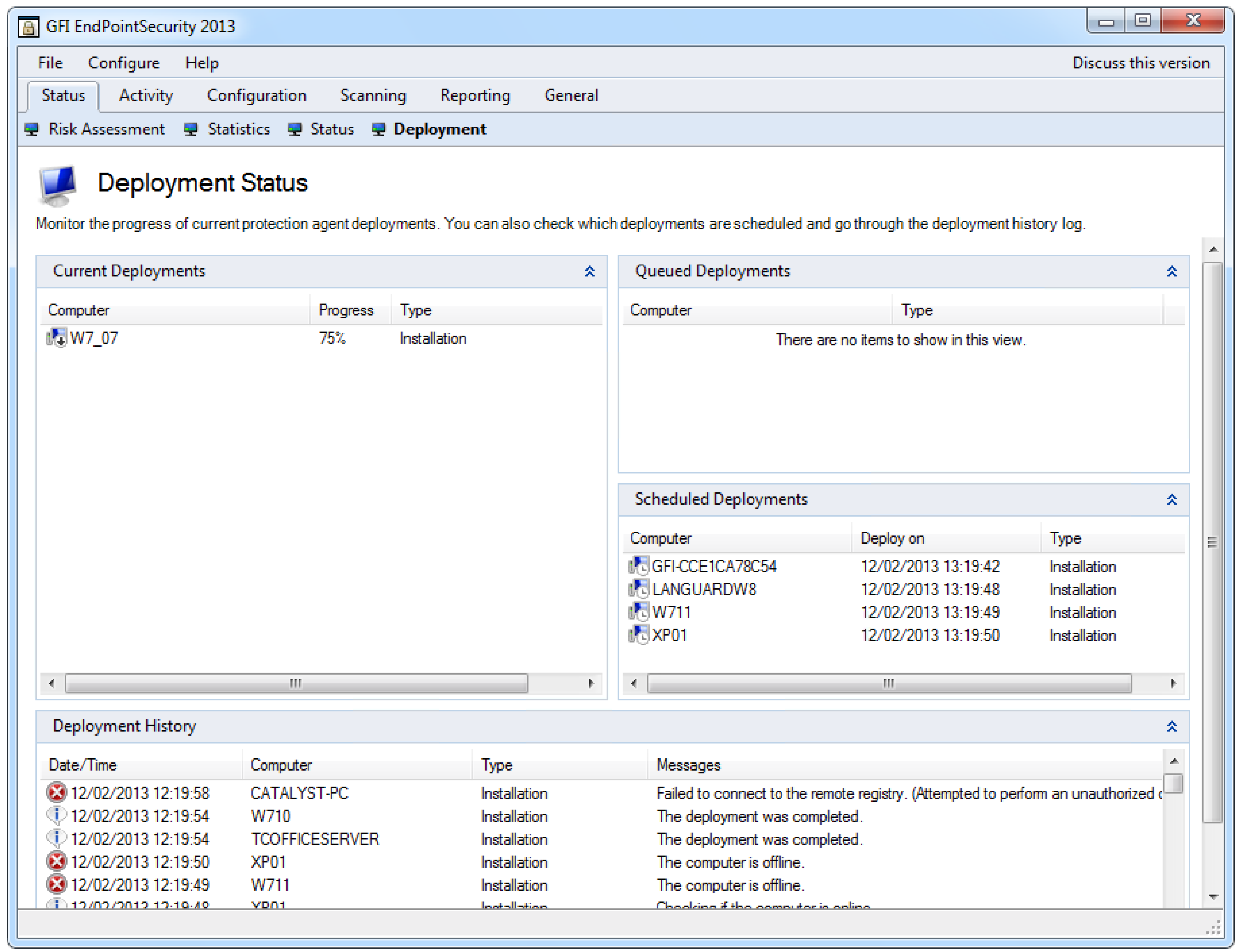
Captura de pantalla 19: Opciones de asignación de directiva de protección

5. En el cuadro de diálogo **Assign Protection Policy**, seleccione la directiva de protección necesaria de la lista desplegable y, a continuación, haga clic en **OK**.

5.2.1 Implementación inmediata

Para implementar de inmediato una directiva de protección en los equipos de destino:

1. Haga clic en la ficha **Configuration** > subficha **Computers**.
2. Resalte los equipos de destino necesarios. Si se requiere más de una implementación, puede resaltar todos los equipos de destino necesarios a la vez y, a continuación, implementar las directivas de protección en el conjunto seleccionado de equipos de destino.
3. En **Actions**, haga clic en **Deploy now...**. La vista debe cambiar automáticamente a **Status** > **Deployment**.

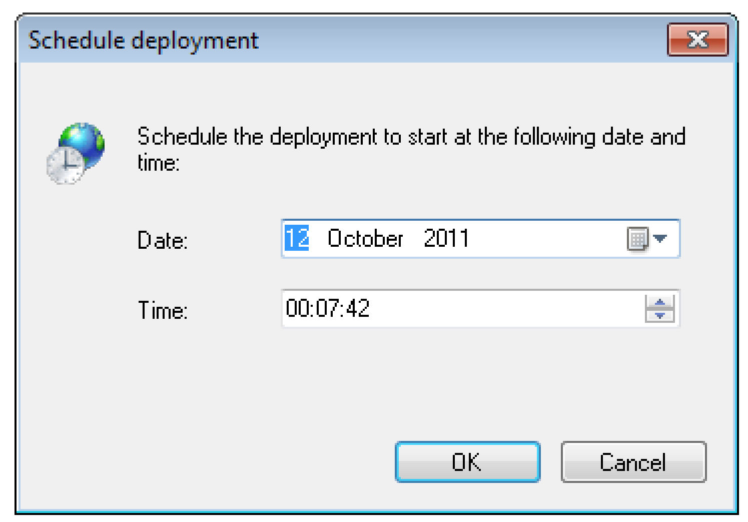


Captura de pantalla 20: Implementación inmediata de una directiva: Subficha Deployment

5.2.2 Implementación programada de directivas

Para programar la implementación de una directiva de protección:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. Resalte los equipos de destino necesarios. Si se requiere más de una implementación, puede resaltar todos los equipos de destino necesarios a la vez y, a continuación, implementar las directivas en el conjunto seleccionado de equipos de destino.
3. En **Actions**, haga clic en **Schedule deployment…**.



Captura de pantalla 21: Opciones de programación de implementaciones

4. En el cuadro de diálogo **Schedule deployment**, seleccione la fecha y hora de implementación y haga clic en **OK**.



Nota

Si el equipo de destino está desconectado, la implementación de la directiva de protección relevante se reprogramará para una hora más tarde. GFI EndPointSecurity sigue intentando implementar esa directiva cada hora, hasta que el equipo de destino se vuelve a conectar.

5.2.3 Implementación de directivas a través de Active Directory

Puede crear un paquete de Windows Installer (archivo de instalación .msi) que después puede implementar a través de directivas de grupo de Active Directory en los equipos de destino de su dominio.

Para crear el paquete de Windows Installer:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En el panel izquierdo, seleccione la directiva de protección para la cual desea crear el paquete de Windows Installer.
3. En la sección **Deployment** del panel derecho, haga clic en **Deploy through Active Directory**.
4. Escriba el **nombre de archivo** del archivo .msi y seleccione la ruta de destino.
5. Haga clic en **Save**.



Nota

Para obtener información sobre cómo implementar software mediante directivas de grupo de Active Directory en Microsoft Windows Server 2003 y Microsoft Windows Server 2008, consulte http://support.microsoft.com/kb/816102.

5.3 Comprobación de la implementación de directivas de protección

Una vez que se implementa una directiva de protección, se recomienda comprobar que la directiva haya afectado los equipos de destino. Compruebe si la implementación se realizó correctamente desde:

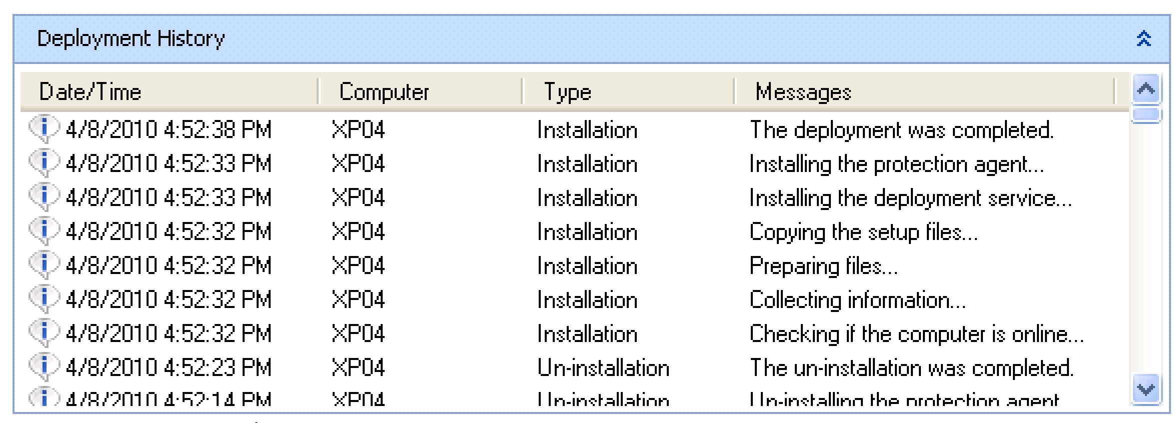
- Área Deployment history
- Área Agents' status

5.3.1 Historial de implementación

Use la información que se muestra en el área Deployment History para determinar si la implementación en cada equipo de destino finalizó correctamente o si se encontraron errores.

Para ver el historial de implementación:

1. Haga clic en **Status> Deployment**.



Deployment History

Date/Time	Computer	Type	Messages
4/8/2010 4:52:38 PM	XP04	Installation	The deployment was completed.
4/8/2010 4:52:33 PM	XP04	Installation	Installing the protection agent...
4/8/2010 4:52:33 PM	XP04	Installation	Installing the deployment service...
4/8/2010 4:52:32 PM	XP04	Installation	Copying the setup files...
4/8/2010 4:52:32 PM	XP04	Installation	Preparing files...
4/8/2010 4:52:32 PM	XP04	Installation	Collecting information...
4/8/2010 4:52:32 PM	XP04	Installation	Checking if the computer is online...
4/8/2010 4:52:23 PM	XP04	Un-installation	The un-installation was completed.
4/8/2010 4:52:14 PM	XP04	Un-installation	Un-installing the protection agent

Captura de pantalla 22: Área Deployment History

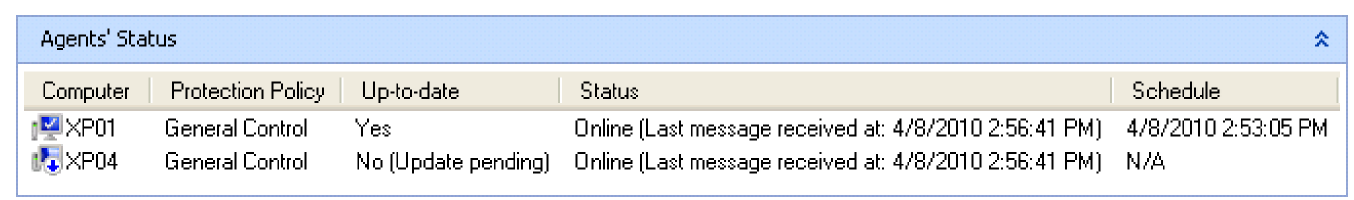
2. En **Deployment History**, confirme que la actualización en el equipo local finalizó correctamente. Para obtener más información, consulte Vista del estado de implementación (página 121).

5.3.2 Estado de agentes

Use la información que se muestra en el área Agents' Status para determinar el estado de todas las operaciones de implementación realizadas en los equipos de destino de su red.

Para ver el estado de los agentes:

3. Haga clic en **Status> Agents**.



Agents' Status

Computer	Protection Policy	Up-to-date	Status	Schedule
XP01	General Control	Yes	Online (Last message received at: 4/8/2010 2:56:41 PM)	4/8/2010 2:53:05 PM
XP04	General Control	No (Update pending)	Online (Last message received at: 4/8/2010 2:56:41 PM)	N/A

Captura de pantalla 23: Área Agent's Status

4. En **Agents' Status**, confirme que la directiva de protección adecuada se haya asignado correctamente a los equipos de destino y que la implementación de agente esté actualizada.



Nota

Cada agente envía su estado en línea a la instalación principal de GFI EndPointSecurity a intervalos regulares. Si la instalación principal no recibe estos datos, el agente se considera desconectado.



Nota

Si un equipo de destino está desconectado, la implementación de la directiva de protección relevante se reprogramará para una hora más tarde. GFI EndPointSecurity sigue intentando implementar esa directiva cada hora, hasta que el equipo de destino se vuelve a conectar.

Para obtener más información acerca del área Agents' Status, consulte la sección Vista del estado de los agentes en el capítulo sobre supervisión de estados.

6 Personalización de directivas de protección

En este capítulo, se proporciona información relacionada con la modificación de los parámetros de sus directivas de protección preconfiguradas. Esto le permite modificar los parámetros con el tiempo, a medida que descubre nuevos obstáculos de seguridad y posibles vulnerabilidades.

Temas de este capítulo

6.1 Configuración de categorías de dispositivos controladas

GFI EndPointSecurity le permite seleccionar qué categorías de dispositivos admitidas debe controlar una directiva de protección. Puede hacer esto directiva por directiva.

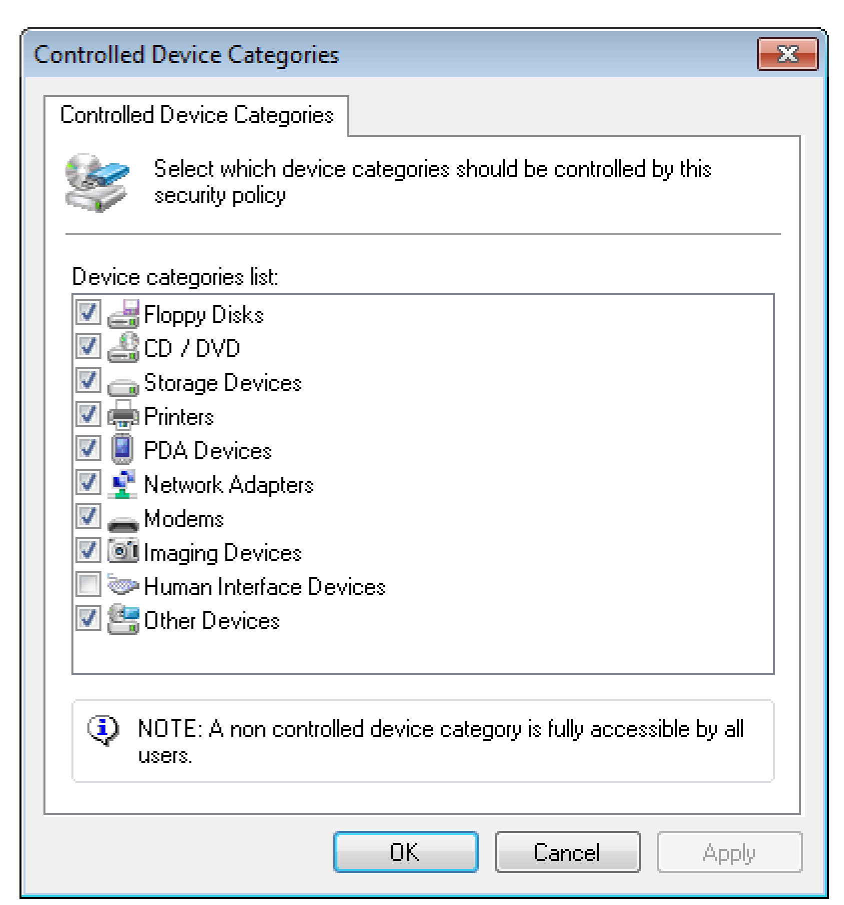


Nota

El acceso completo a los dispositivos no especificados es posible desde los equipos de destino abarcados por la directiva de protección. Como resultado, GFI EndPointSecurity no puede supervisar ni bloquear dispositivos incluidos en una categoría que no esté controlada por la directiva de protección.

Para configurar dispositivos controlados a través de una directiva de protección:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. Haga clic en **Security**.
4. En **Common tasks**, haga clic en **Edit controlled device categories...**.



Captura de pantalla 24: Opciones de categorías de dispositivos controladas

5. En el cuadro de diálogo **Controlled Device Categories**, seleccione o anule la selección de las categorías de dispositivos que se controlarán con la directiva de protección y haga clic en **OK**.



Importante

Si habilita dispositivos de interfaz humana y rechaza el acceso a estos dispositivos, los usuarios no podrán usar ratones y teclados USB conectados a los equipos de destino protegidos por esta directiva.

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Deploy to all computers...**.

6.2 Configuración de puertos de conectividad controlados

GFI EndPointSecurity le permite seleccionar qué puertos de conectividad admitidos debe controlar una directiva de protección. Puede hacer esto directiva por directiva.

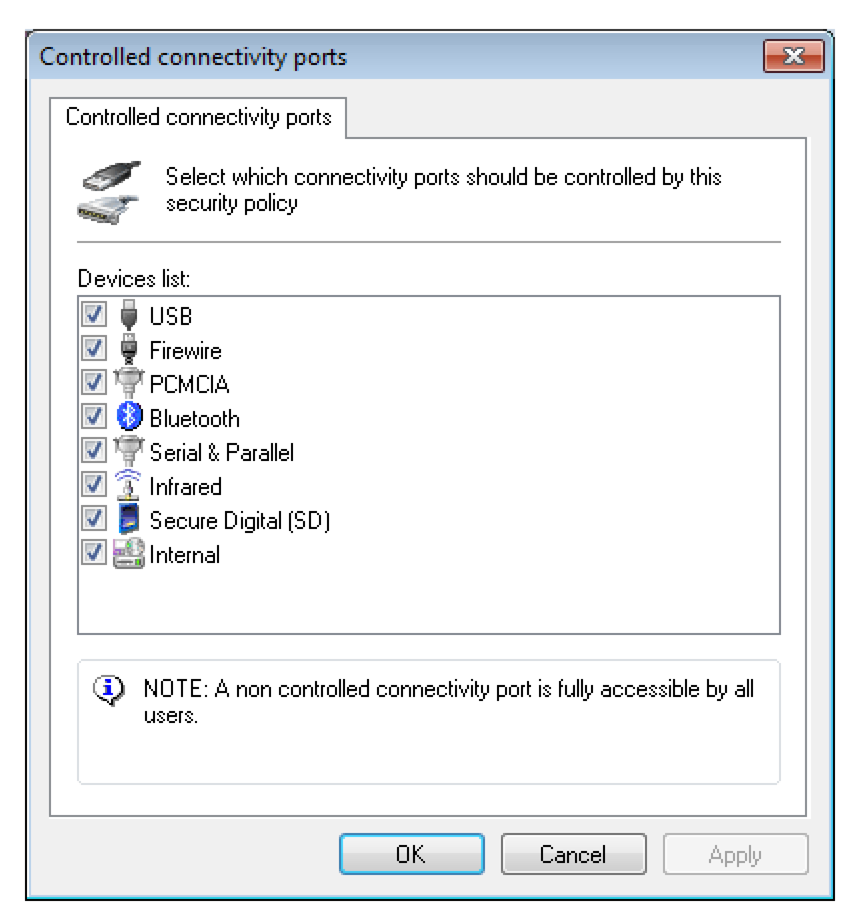


Nota

El acceso completo a los puertos no especificados es posible desde los equipos de destino abarcados por la directiva de protección. Como resultado, GFI EndPointSecurity no puede supervisar ni bloquear dispositivos conectados a un puerto que no esté controlado por la directiva de protección.

Para configurar qué puertos se controlarán a través de una directiva de protección específica:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. Haga clic en **Security**.
4. En **Common tasks**, haga clic en **Edit controlled ports...**.



Captura de pantalla 25: Opciones de puertos de conectividad controlados

5. En el cuadro de diálogo **Controlled connectivity ports**, seleccione o anule la selección de los puertos de conectividad necesarios que se controlarán con la directiva de protección y haga clic en **OK**.

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Deploy to all computers...**.

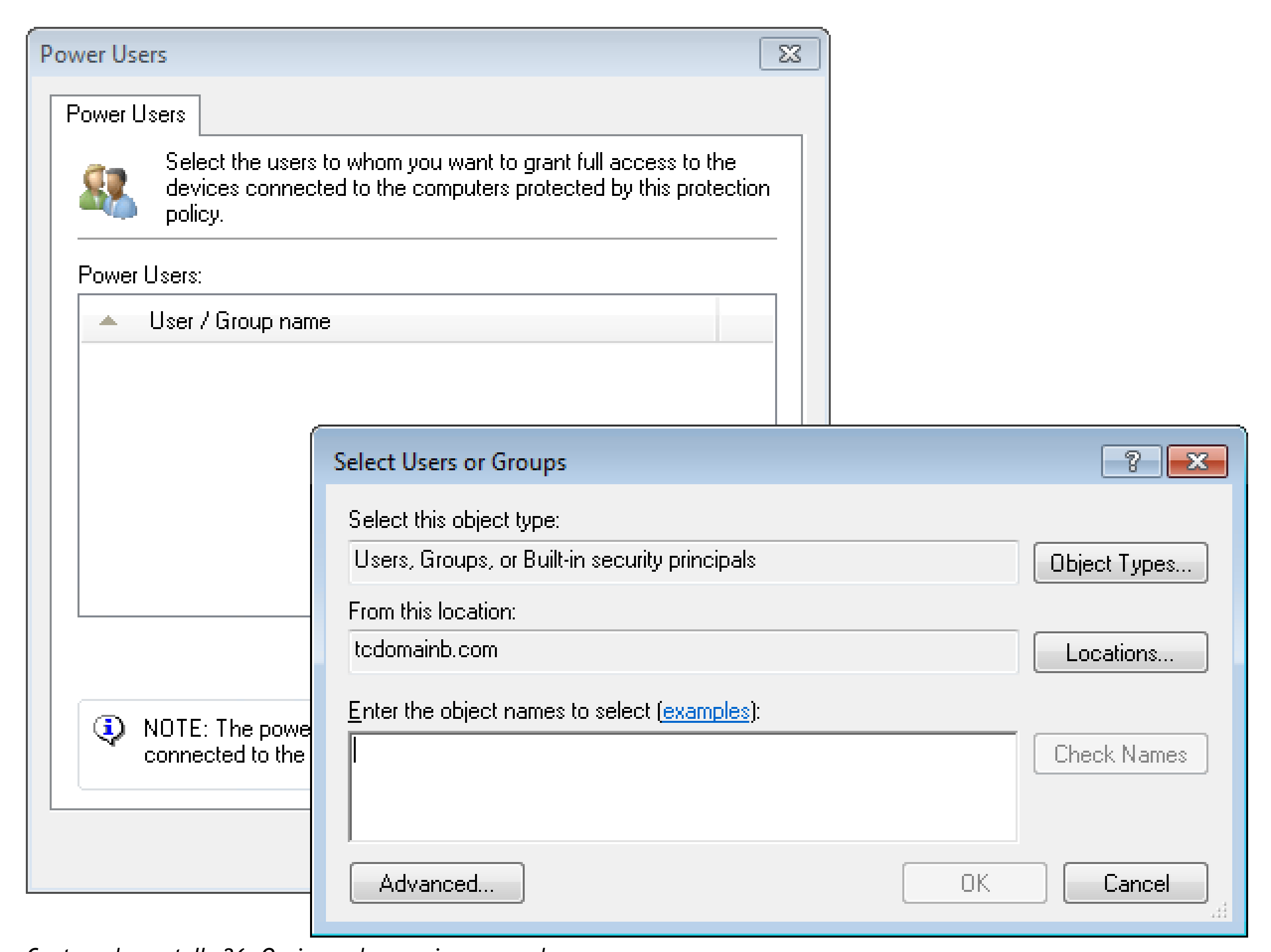
6.3 Configuración de usuarios avanzados

GFI EndPointSecurity le permite especificar usuarios o grupos de usuarios de Active Directory (AD) como usuarios avanzados. Los usuarios avanzados obtienen acceso total a los dispositivos conectados a cualquier equipo de destino abarcado por una directiva de protección. Puede definir conjuntos de usuarios avanzados directiva por directiva.

Debe tener precaución al usar esta función, dado que especificar incorrectamente un usuario como usuario avanzado provocará que el usuario invalide todas las restricciones de la directiva de protección relevante.

Para especificar usuarios avanzados de una directiva de protección:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. En la sección **Security** del panel derecho, haga clic en **Power users**.



Captura de pantalla 26: Opciones de usuarios avanzados

4. En el cuadro de diálogo Power Users:

- **Opción 1**: Haga clic en **Add...** para especificar los grupos de usuarios que se establecerán como usuarios avanzados de esta directiva de protección y, a continuación, haga clic en **OK**.
- **Opción 2**: Resalte los grupos de usuarios y haga clic en **Remove** para bajar el nivel de los usuarios avanzados; a continuación, haga clic en **OK**.

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Deploy to all computers…**.

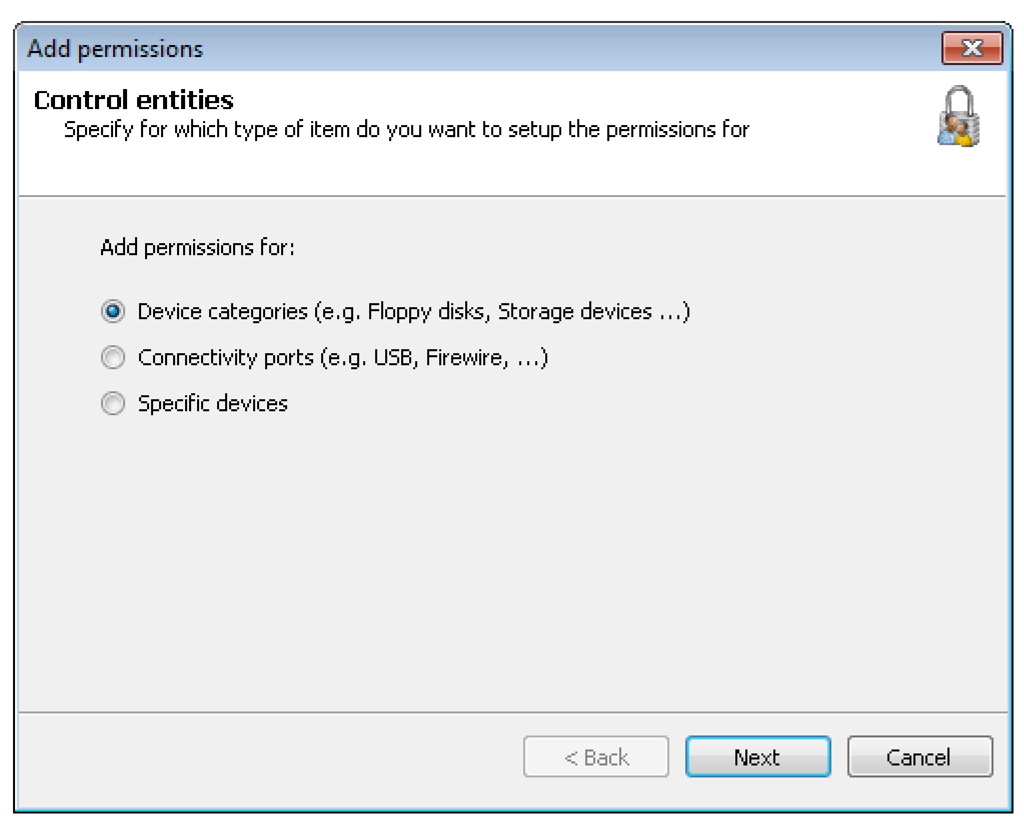
6.4 Configuración de permisos de acceso para categorías de dispositivos

GFI EndPointSecurity le permite establecer permisos por categorías de dispositivos para los usuarios o grupos de usuarios de Active Directory (AD). Puede hacer esto directiva por directiva.

Cuando una categoría de dispositivo no se configura para que la controle una directiva de seguridad en particular, se deshabilita la entrada relevante. Para obtener más información, consulte Configuración de categorías de dispositivos controladas (página 59).

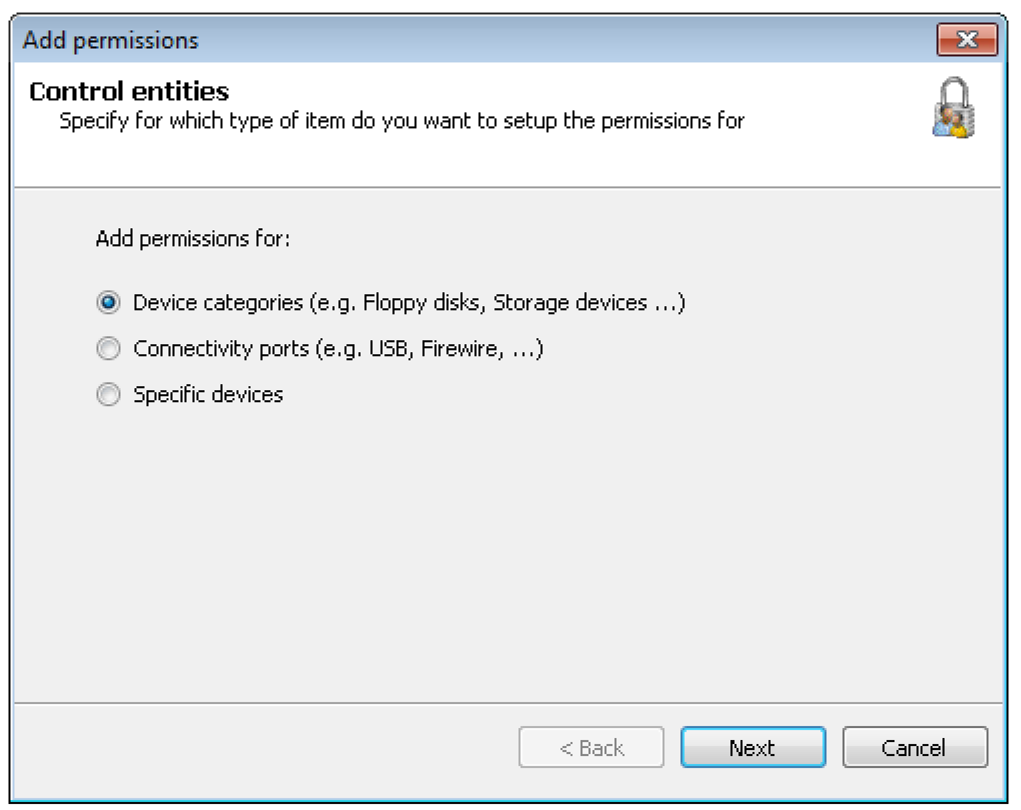
Para configurar permisos de acceso de categorías de dispositivos para los usuarios en una directiva de protección:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. En **Common tasks**, haga clic en **Add permission(s)…**.



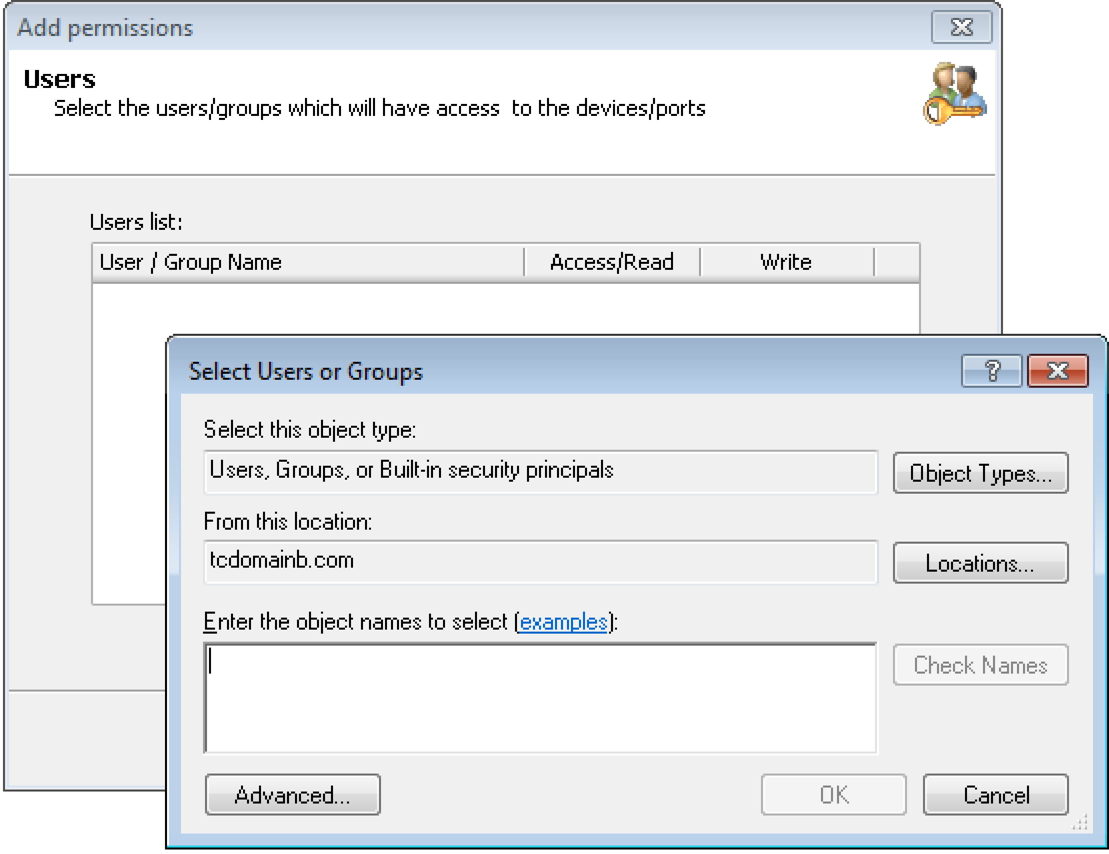
Captura de pantalla 27: Opciones de incorporación de permisos: Entidades de control

4. En el cuadro de diálogo **Add permissions**, seleccione **Device categories** y haga clic en **Next**.



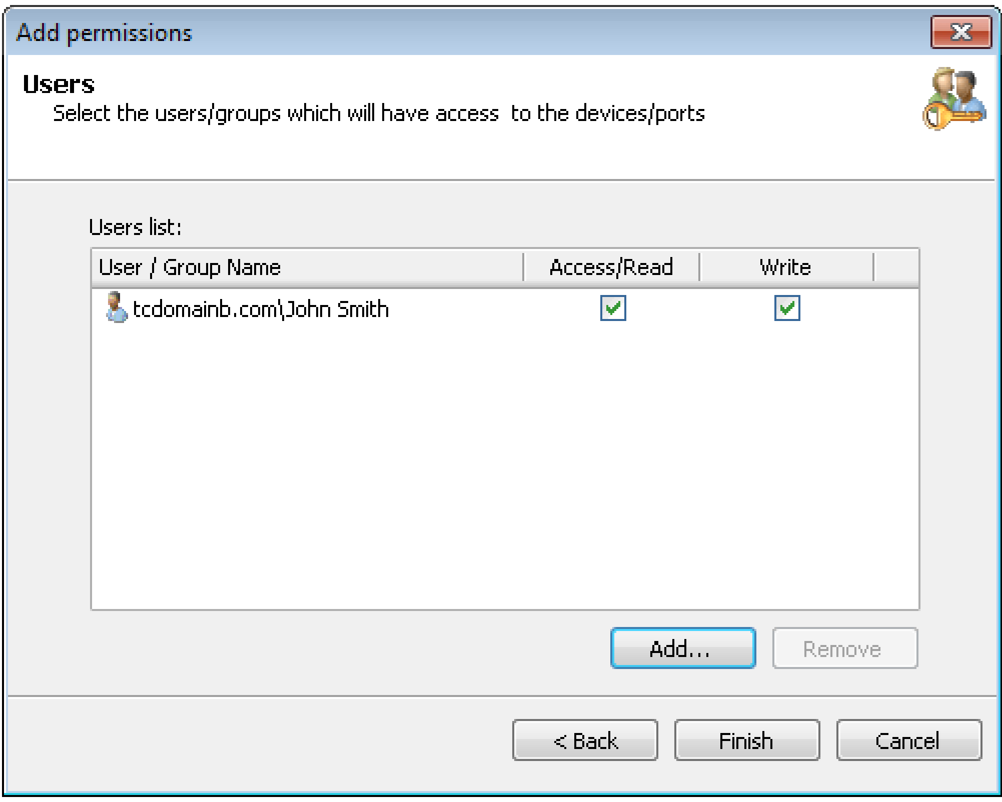
Captura de pantalla 28: Opciones de incorporación de permisos: Categorías de dispositivos

5. Habilite o deshabilite las categorías de dispositivos necesarias para las cuales desee configurar permisos y haga clic en **Next**.



Captura de pantalla 29: Opciones de incorporación de permisos: Usuarios

6. Haga clic en **Add...** para especificar los grupos de usuarios que tendrán acceso a las categorías de dispositivos especificadas en esta directiva de protección y haga clic en **OK**.



Captura de pantalla 30: Opciones de incorporación de permisos: Usuarios

7. Habilite o deshabilite los permisos de acceso/lectura y escritura para cada usuario o grupo especificado, y haga clic en **Finish**.

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Deploy to all computers...**.

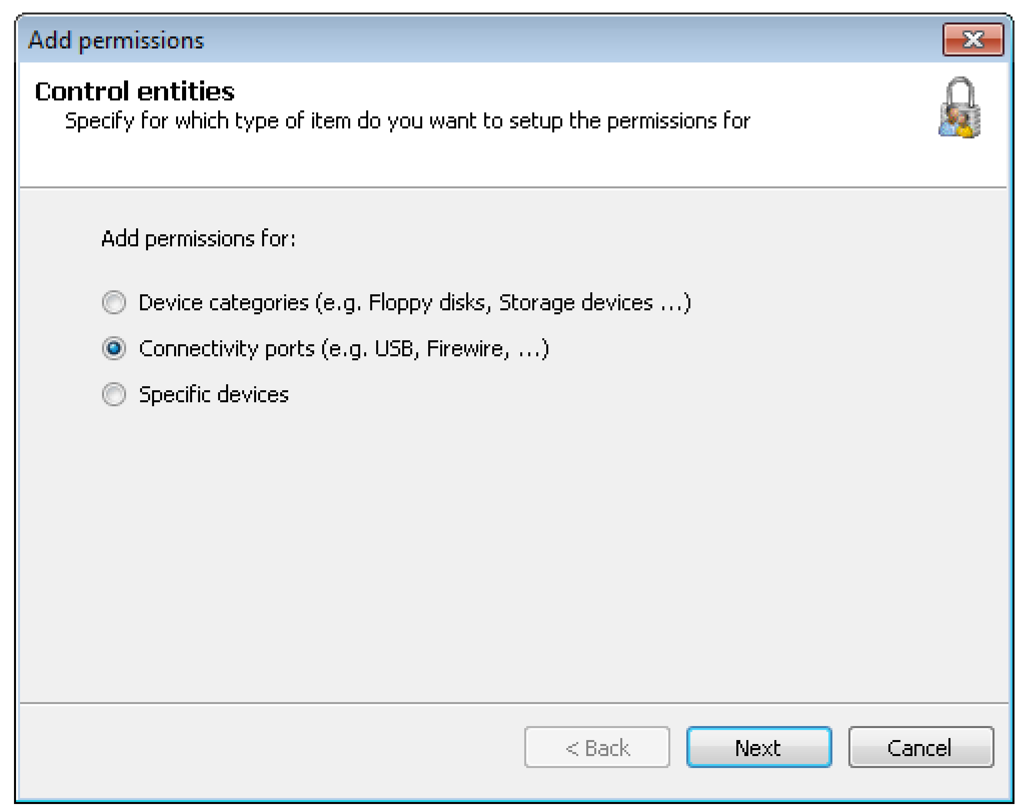
6.5 Configuración de permisos de acceso para puertos de conectividad

GFI EndPointSecurity le brinda la facilidad de establecer permisos por puertos de conectividad para los usuarios o grupos de usuarios de Active Directory (AD). Puede hacer esto directiva por directiva.

Cuando un puerto de conectividad no está configurado para que lo controle una directiva de protección, se deshabilita el permiso relevante. Para obtener más información, consulte Configuración de puertos de conectividad controlados (página 61).

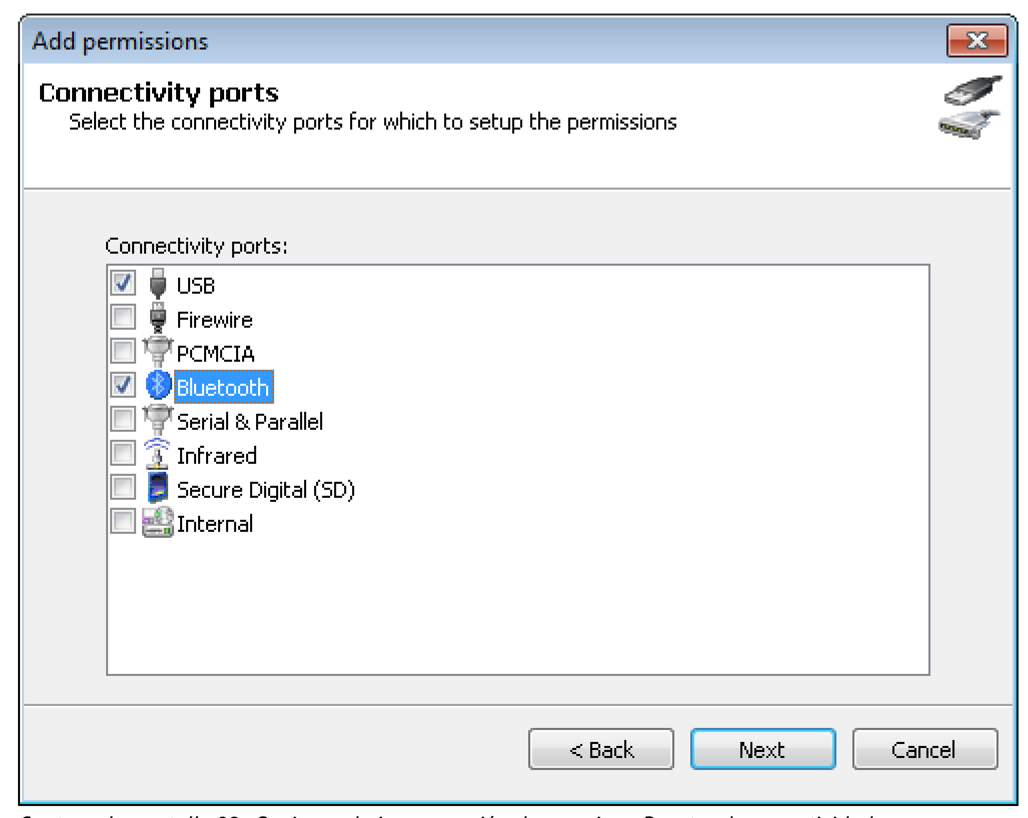
Para configurar los permisos de uso de los puertos de conectividad para los usuarios dentro de una directiva de protección específica:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. Haga clic en **Security** > **Set Permissions**.
4. En **Common tasks**, haga clic en **Add permission(s)...**.



Captura de pantalla 31: Opciones de incorporación de permisos: Entidades de control

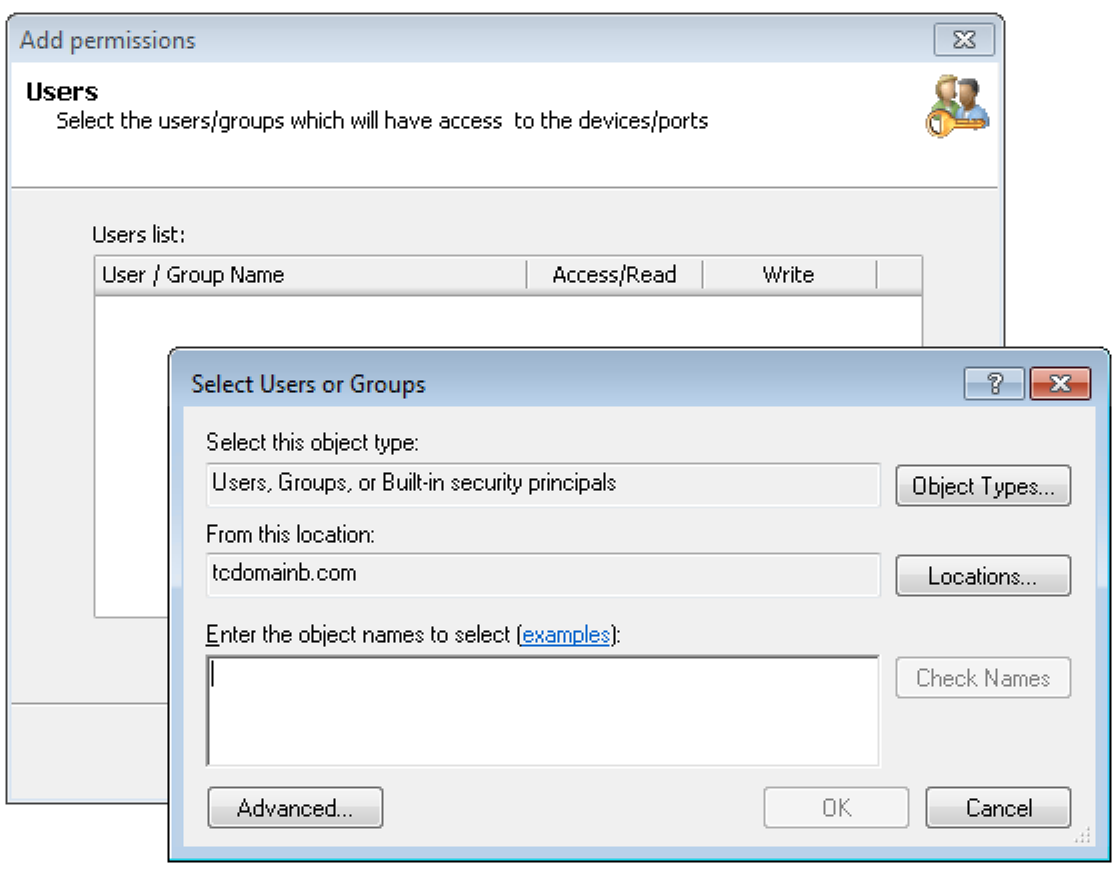
5. En el cuadro de diálogo **Add permissions**, seleccione **Connectivity ports** y haga clic en **Next**.



Captura de pantalla 32: Opciones de incorporación de permisos: Puertos de conectividad

6. Habilite o deshabilite los puertos de conectividad necesarios para los cuales desee configurar permisos y haga clic en **Next**.

7. Haga clic en **Add...** para especificar los grupos de usuarios que tendrán acceso a los puertos de conectividad especificados en esta directiva de protección y haga clic en **OK**.



Captura de pantalla 33: Opciones de incorporación de permisos: Usuarios

8. Habilite o deshabilite los permisos de acceso/lectura para cada usuario o grupo especificado, y haga clic en **Finish**.

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Deploy to all computers...**.

6.6 Configuración de permisos de acceso para dispositivos específicos

GFI EndPointSecurity le permite establecer permisos por dispositivos específicos para los usuarios o grupos de usuarios de Active Directory (AD). Puede hacer esto directiva por directiva.

Por ejemplo, puede asignar permisos de solo lectura a un pen drive USB aprobado de una compañía específica. Se bloquearán los intentos de usar otros pen drives USB no aprobados.

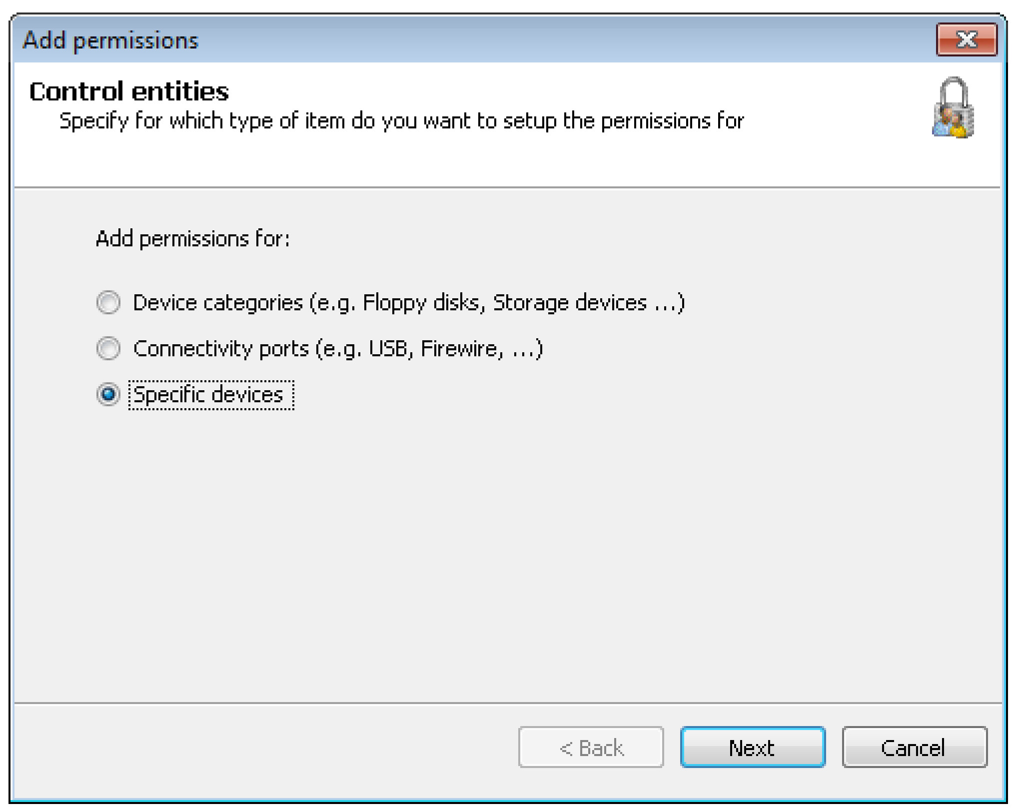


Nota

Para obtener una lista actualizada de los dispositivos actualmente conectados a los equipos de destino, ejecute un examen de equipos y agregue los dispositivos detectados a la base de datos de dispositivos antes de configurar permisos de acceso para dispositivos específicos. Para obtener más información, consulte Detección de dispositivos (página 102).

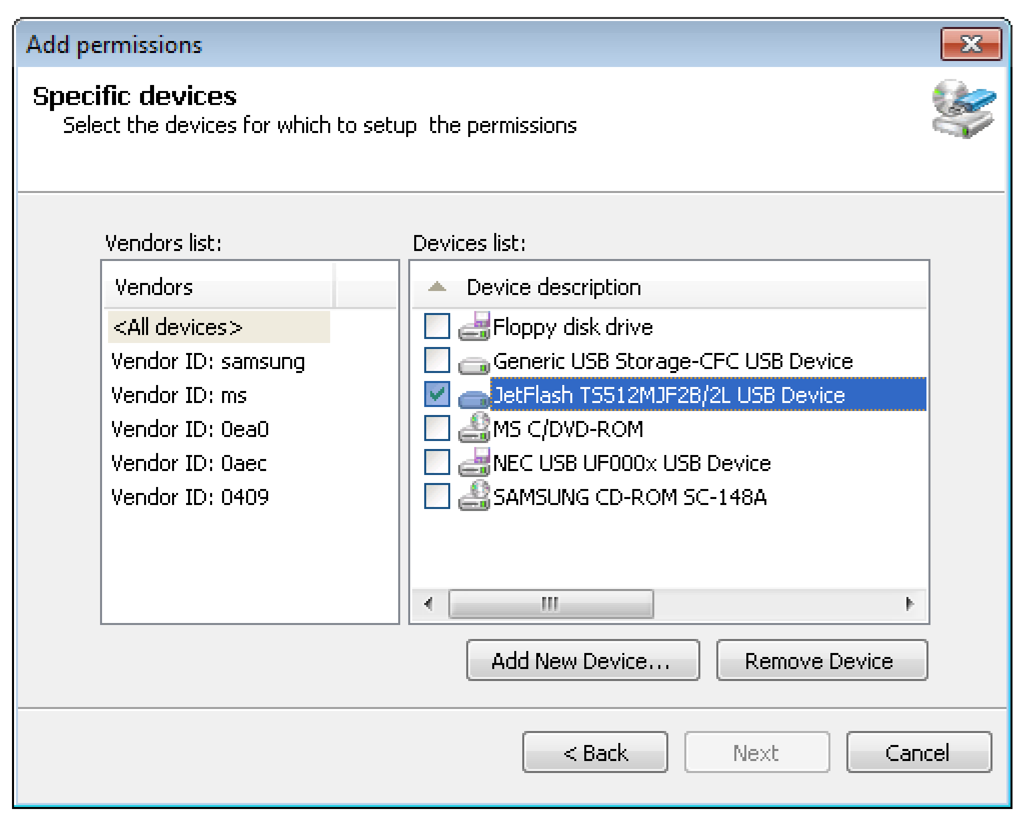
Para configurar permisos de acceso para dispositivos específicos para los usuarios de una directiva de protección:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. Haga clic en el subnodo **Security**.
4. En la sección **Common tasks** del panel izquierdo, haga clic en **Add permission(s)...**.



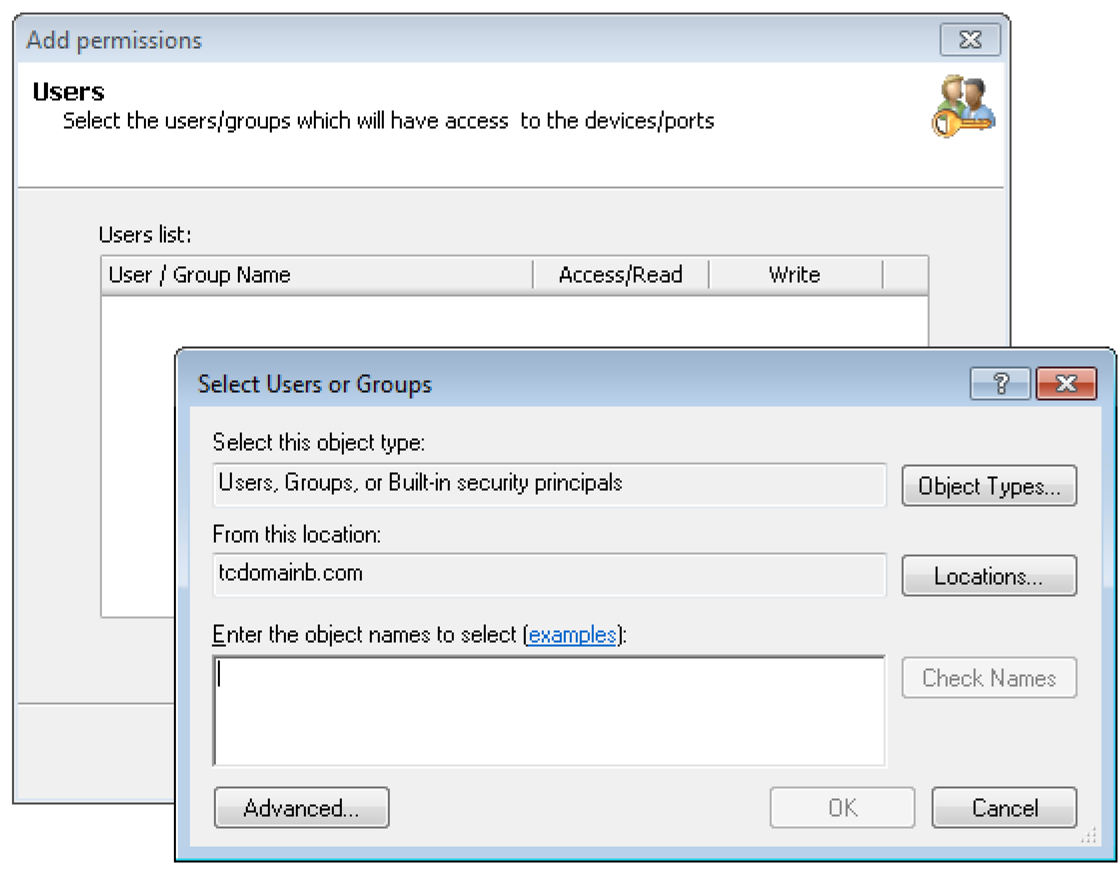
Captura de pantalla 34: Opciones de incorporación de permisos: Entidades de control

5. En el cuadro de diálogo **Add permissions**, seleccione **Specific devices** y haga clic en **Next**.



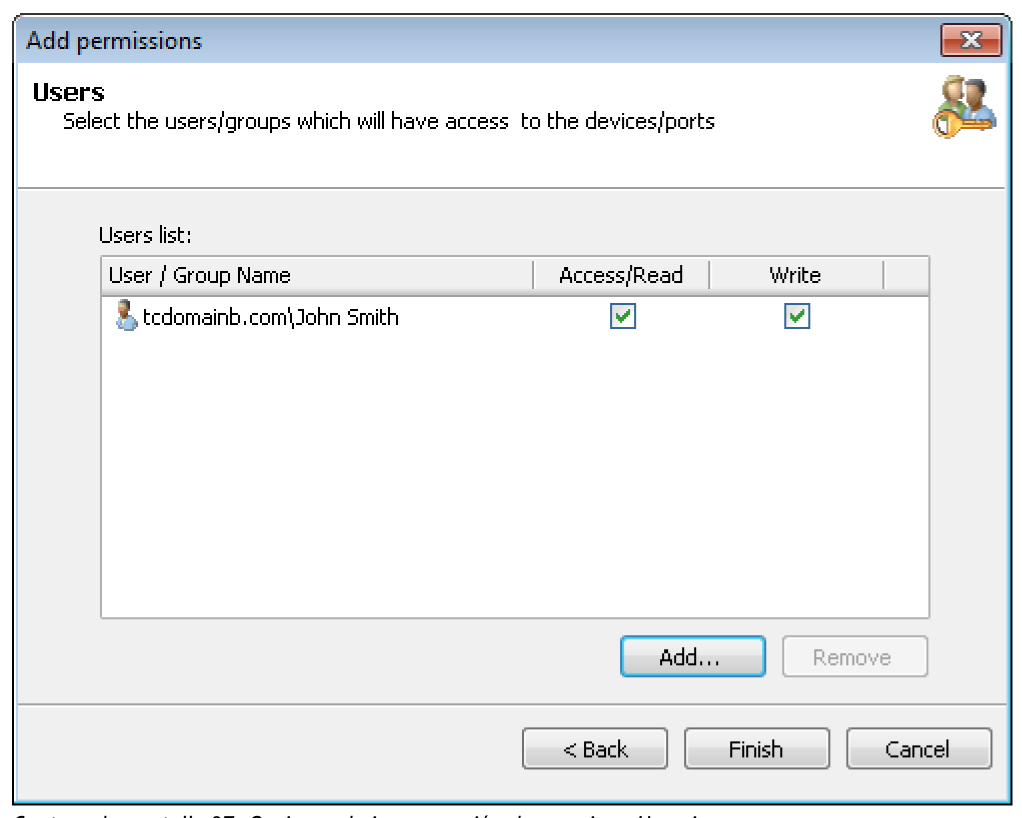
Captura de pantalla 35: Opciones de incorporación de permisos: Dispositivos específicos

6. Habilite o deshabilite los dispositivos necesarios de la lista Devices para los cuales desee configurar permisos y haga clic en **Next**. Si un dispositivo necesario no está incluido en la lista, haga clic en **Add New Device…** para especificar los detalles del dispositivo para el cual desea configurar permisos y haga clic en **OK**.



Captura de pantalla 36: Opciones de incorporación de permisos: Usuarios

7. Haga clic en **Add…** para especificar los grupos de usuarios que tendrán acceso a los dispositivos especificados en esta directiva de protección y, a continuación, haga clic en **OK**.



Captura de pantalla 37: Opciones de incorporación de permisos: Usuarios

8. Habilite o deshabilite los permisos de acceso/lectura y escritura para cada usuario o grupo especificado, y haga clic en **Finish**.

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Deploy to all computers...**.

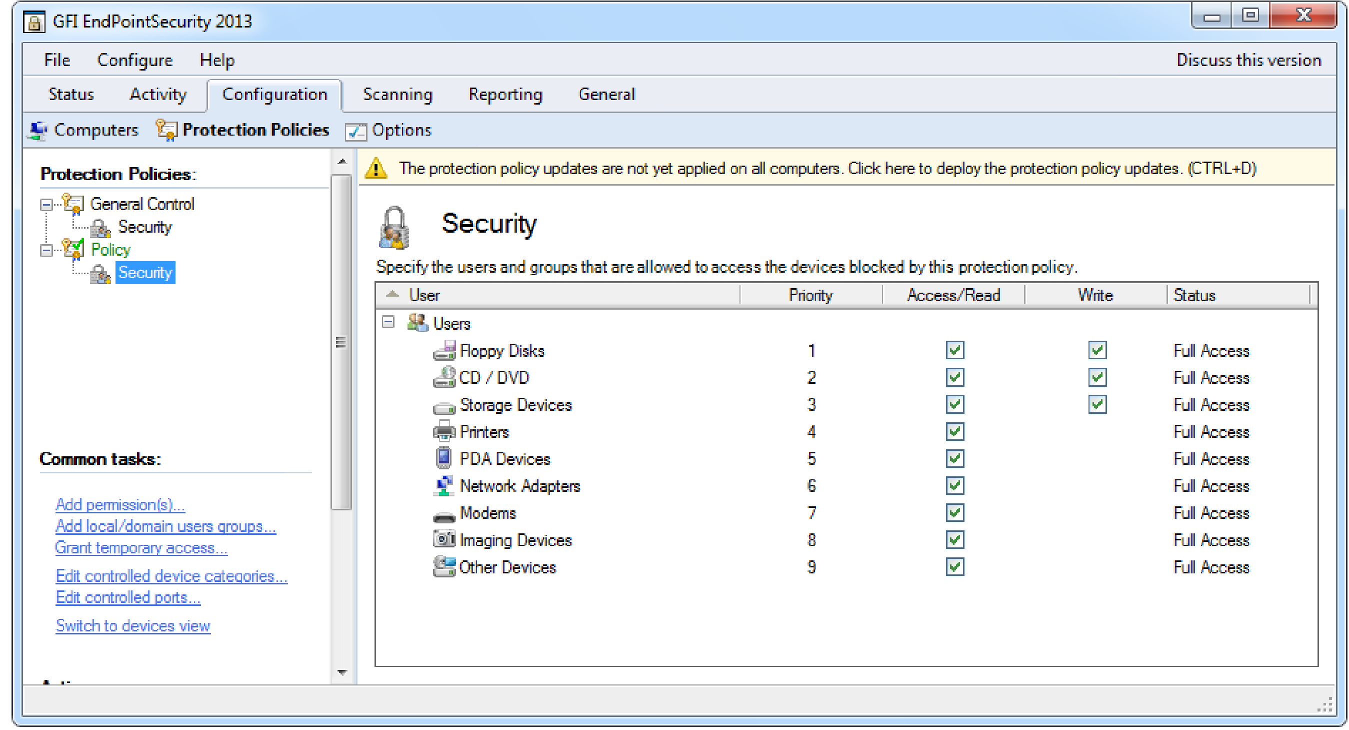
6.7 Visualización de permisos de acceso

GFI EndPointSecurity le permite ver todos los permisos asignados a usuarios o grupos de usuarios de Active Directory (AD). Puede hacer esto directiva por directiva.

Cuando una categoría de dispositivo o un puerto de conectividad no están configurados para que los controle una directiva de seguridad en particular, se deshabilita el permiso relevante. Para obtener más información, consulte Configuración de categorías de dispositivos controladas o Configuración de puertos de conectividad controlados.

Para ver todos los permisos asignados a usuarios en una directiva de protección:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. Haga clic en **Security**. En el panel derecho, puede ver todos los permisos establecidos para esta directiva de protección.



Captura de pantalla 38: Subficha Protection Policies: Vista de dispositivos

Captura de pantalla 39: Subficha Protection Policies: Vista de usuarios

4. En la sección **Common tasks** del panel izquierdo, haga clic en **Switch to devices view** o **Switch to users view** para cambiar la agrupación de permisos por dispositivos/puertos o usuarios.



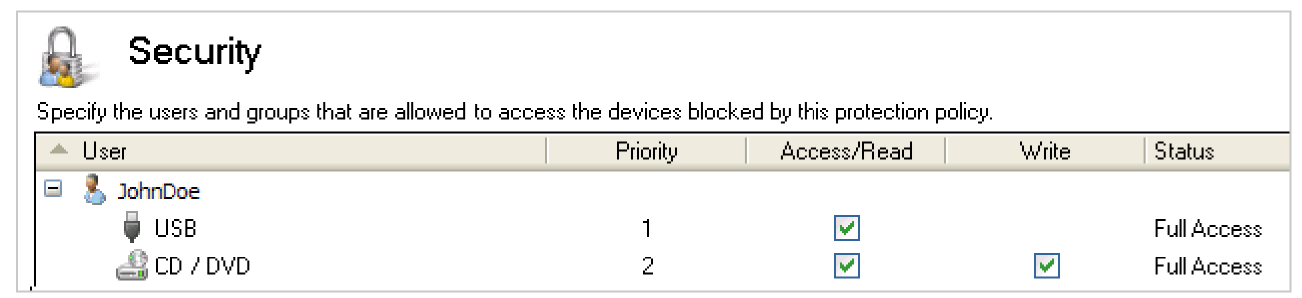
Nota

El la vista de usuarios, también podrá ver los usuarios avanzados especificados en la directiva.

6.8 Configuración de prioridades de permisos

GFI EndPointSecurity le permite priorizar los permisos asignados a usuarios o grupos de usuarios de Active Directory (AD). Puede hacer esto directiva por directiva o usuario por usuario.

Por ejemplo, para un usuario en particular especificado dentro de una directiva de protección determinada, puede decidir darle prioridad 1 a los permisos de puertos USB y prioridad 2 a los permisos de unidades de CD/DVD. Esto significa que si el usuario conecta una unidad de CD/DVD externa a través del puerto USB al equipo de destino, los permisos para el puerto USB tendrán prioridad sobre los permisos para la unidad de CD/DVD.



Captura de pantalla 40: Subficha Protection Policies: Área Security

Para priorizar los permisos asignados a usuarios en una directiva de protección:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. Haga clic en el subnodo **Security**.
4. En la sección **Common tasks** del panel izquierdo, haga clic en **Switch to users view** para cambiar la agrupación de permisos por usuarios.
5. Haga clic con el botón secundario en la sección **Security** y seleccione **Expand all**.
6. Resalte el dispositivo o puerto necesario.
7. En la sección **Actions** del panel izquierdo, haga clic en **Increase priority** o en **Decrease priority**.

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Deploy to all computers…**.

6.9 Configuración de una lista negra de dispositivos

GFI EndPointSecurity le permite especificar qué dispositivos pueden volverse inaccesibles para todos. La lista negra es granular, de manera que puede incluir hasta un dispositivo específico con un número de serie determinado. Puede hacer esto directiva por directiva.

Para obtener una lista actualizada de los dispositivos actualmente conectados a los equipos de destino, ejecute un examen de dispositivos y agregue los dispositivos detectados a la base de datos de dispositivos antes de configurar los dispositivos de la lista negra. Para obtener más información, consulte Detección de dispositivos (página 102).

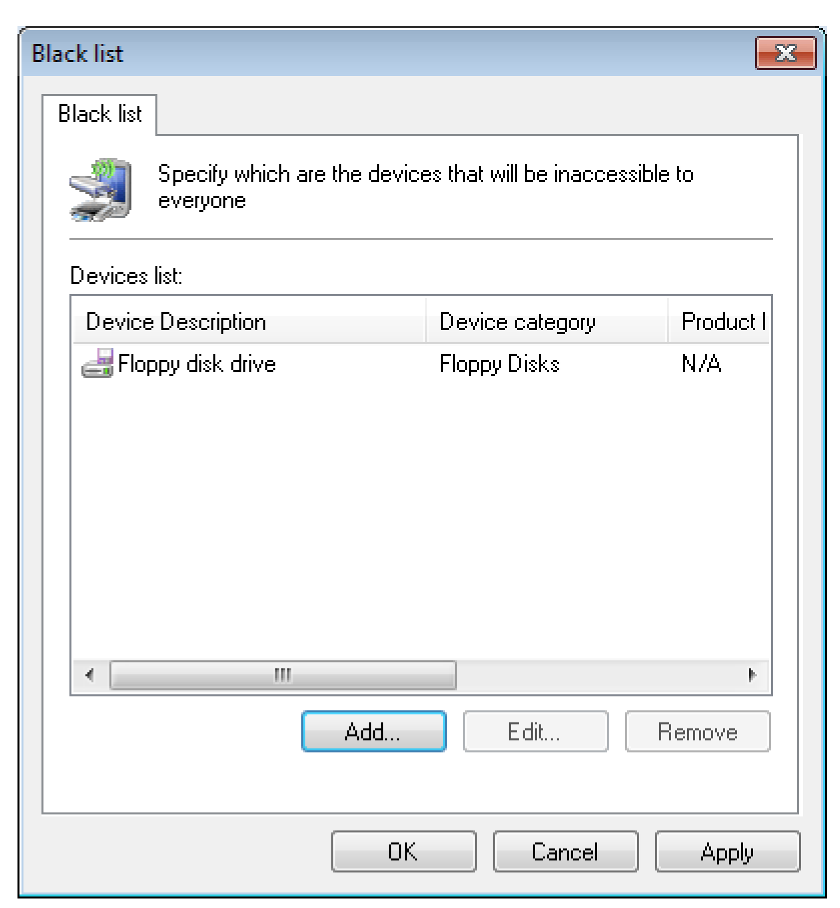


Nota

Los usuarios avanzados invalidarán los dispositivos de la lista negra y, de este modo, podrán acceder a esos dispositivos.

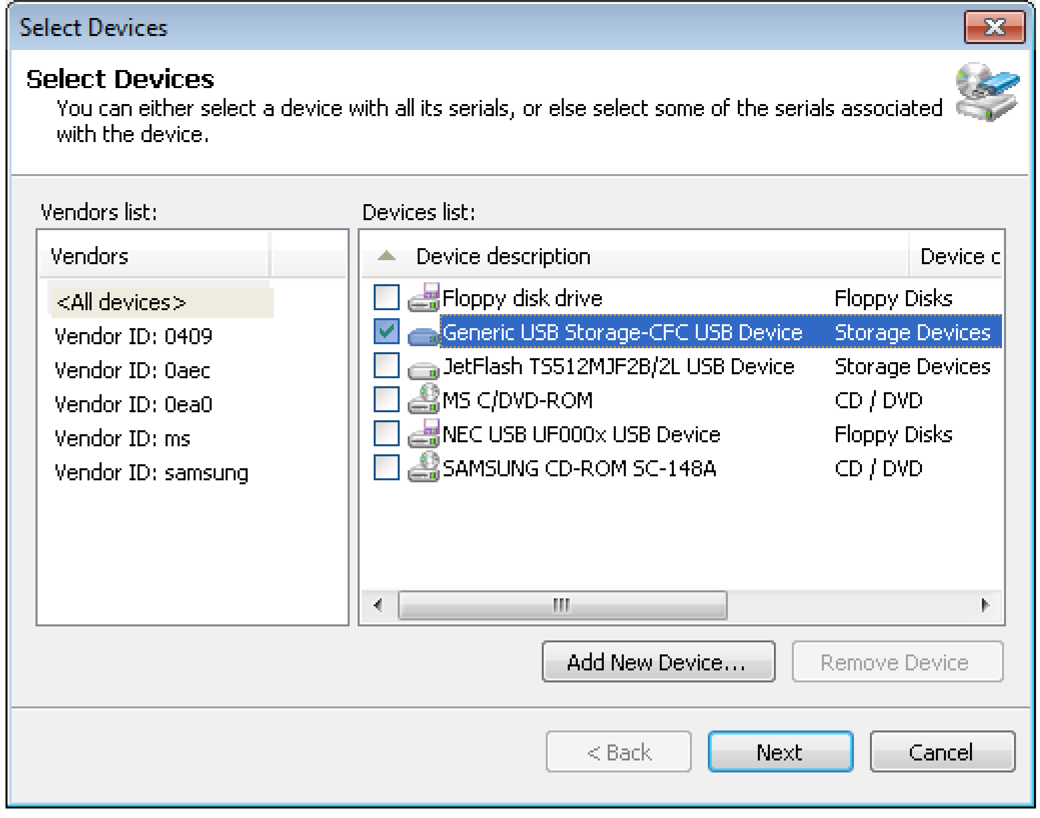
Para agregar dispositivos a la lista negra de una directiva de protección específica:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. En la sección **General Control** del panel derecho, haga clic en **Devices Blacklist**.



Captura de pantalla 41: Opciones de lista negra

4. En el cuadro de diálogo **Black list**, haga clic en **Add…** para seleccionar los dispositivos que desee agregar a la lista negra.



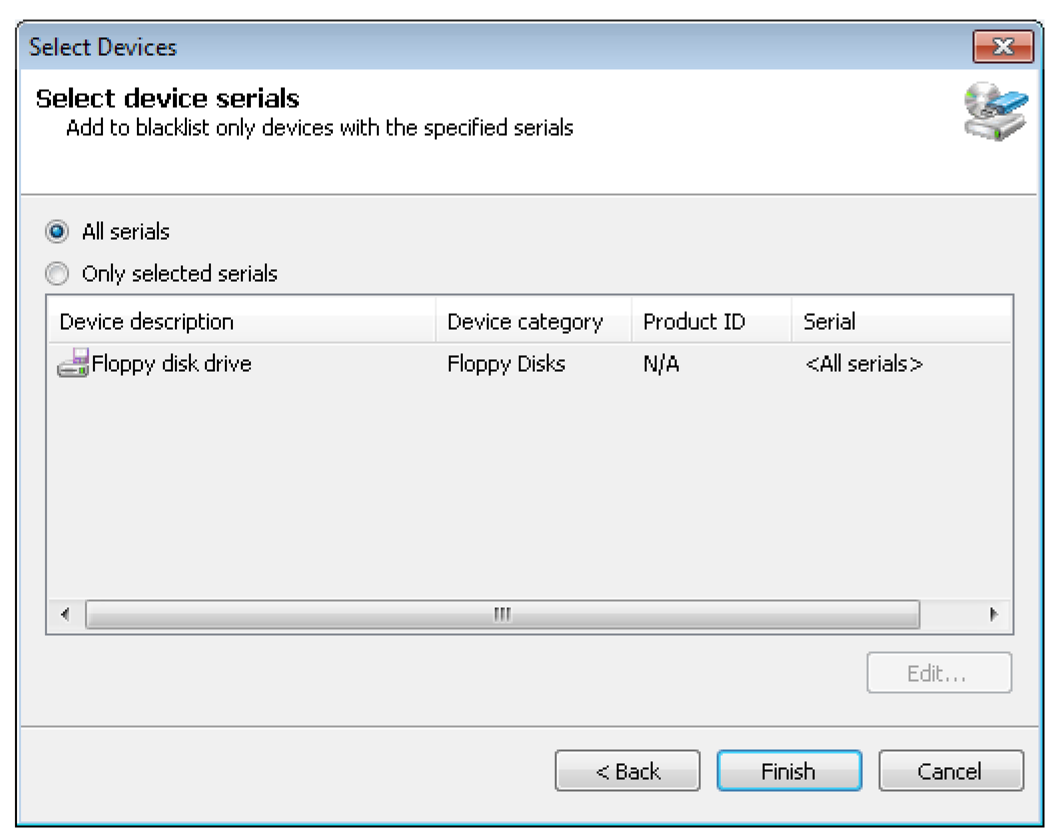
Captura de pantalla 42: Opciones de selección de dispositivos

5. En el cuadro de diálogo **Select Devices**, habilite o deshabilite los dispositivos para agregar a la lista negra desde la lista Devices y haga clic en **Next**.



Nota

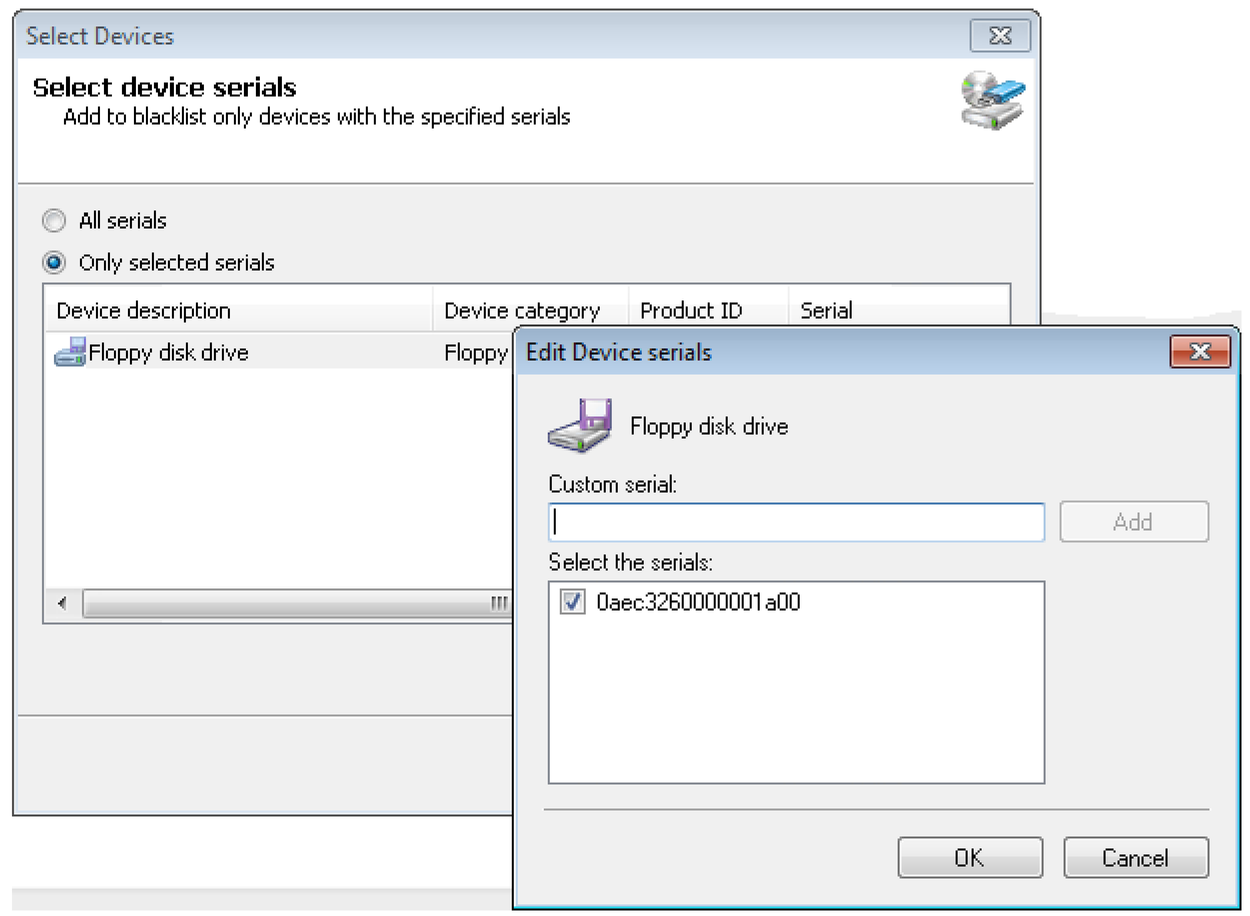
Si un dispositivo necesario no está incluido en la lista, haga clic en **Add New Device...** para especificar los detalles del dispositivo que desea agregar a la lista negra y haga clic en **OK**.



Captura de pantalla 43: Opciones de selección de dispositivos: Select device serials

6. Seleccione la opción relacionada con los números de serie necesarios entre:

- **All serials**: para incluir en la lista negra todos los número de serie de un dispositivo específico. Haga clic en **Finish** y en **OK**.
- **Only selected serials**: para especificar números de serie de dispositivos particulares para que se agreguen a la lista negra. A continuación, resalte el dispositivo y haga clic en **Edit...** para especificar los números de serie. Haga clic en **OK**, en **Finish** y en **OK**.



Captura de pantalla 44: Opciones de selección de dispositivos: Edit Device serials

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Deploy to all computers...**.

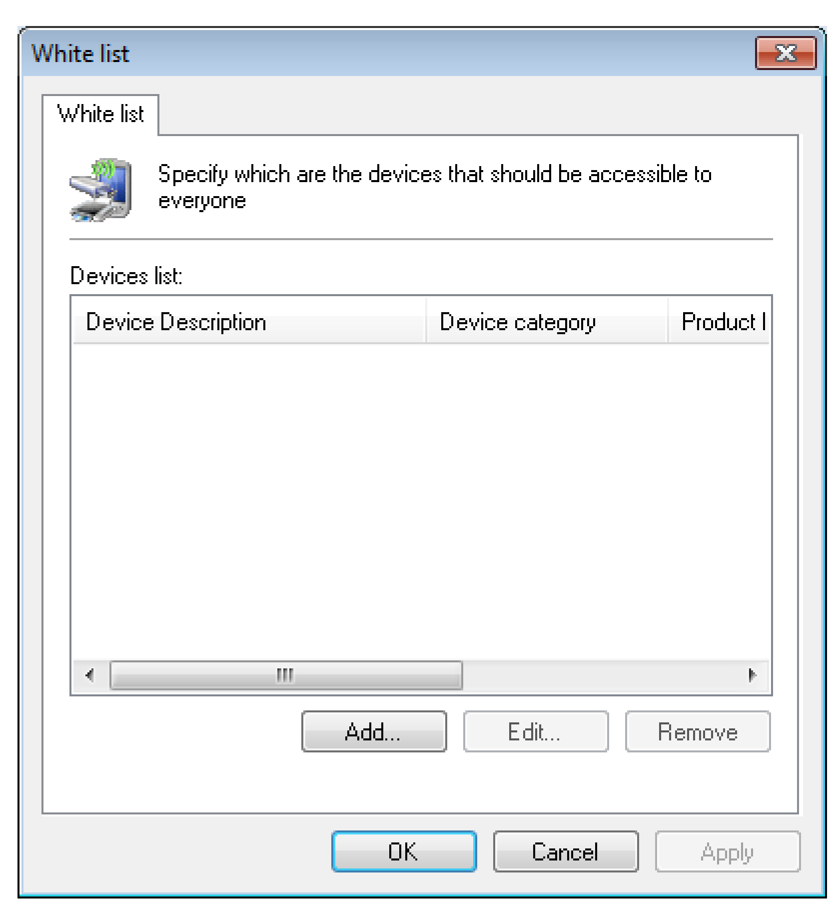
6.10 Configuración de una lista blanca de dispositivos

GFI EndPointSecurity le permite especificar a qué dispositivos pueden acceder todos. La lista blanca es granular, de manera que puede incluir hasta un dispositivo específico con un número de serie determinado. Puede hacer esto directiva por directiva.

Para obtener una lista actualizada de los dispositivos actualmente conectados a los equipos de destino, ejecute un examen de dispositivos y agregue los dispositivos detectados a la base de datos de dispositivos antes de configurar los dispositivos de la lista blanca. Para obtener más información, consulte Detección de dispositivos (página 102).

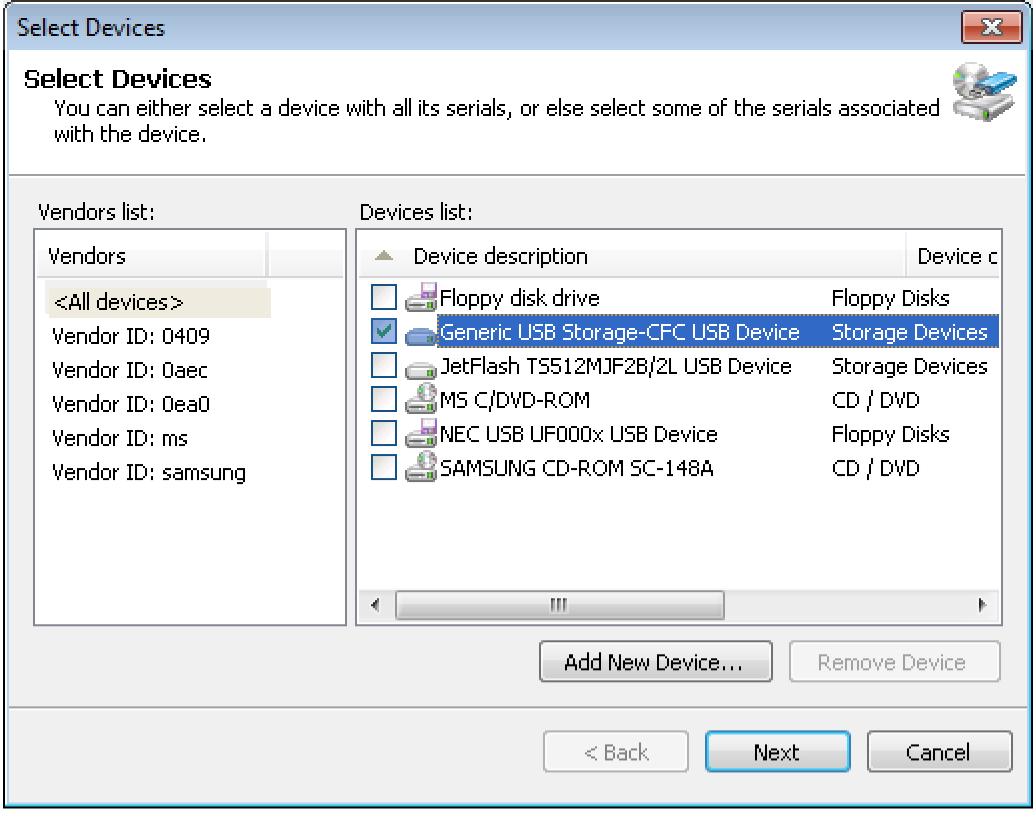
Para agregar dispositivos de lista blanca a una directiva de protección:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. En la sección **General Control** del panel derecho, haga clic en **Devices WhiteList**.



Captura de pantalla 45: Opciones de lista blanca

4. En el cuadro de diálogo **White list**, haga clic en **Add...** para seleccionar los dispositivos que desee agregar a la lista blanca.



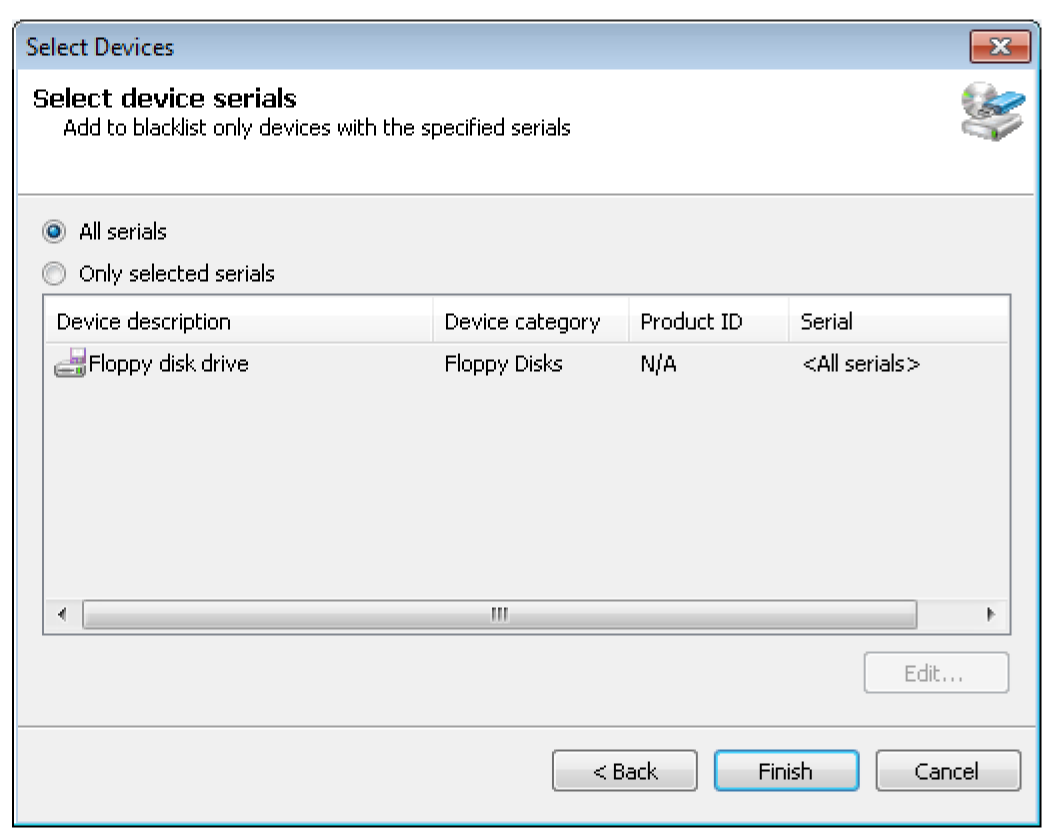
Captura de pantalla 46: Opciones de selección de dispositivos

5. En el cuadro de diálogo **Select Devices**, habilite o deshabilite los dispositivos para agregar a la lista blanca desde la lista Devices y haga clic en **Next**.



Nota

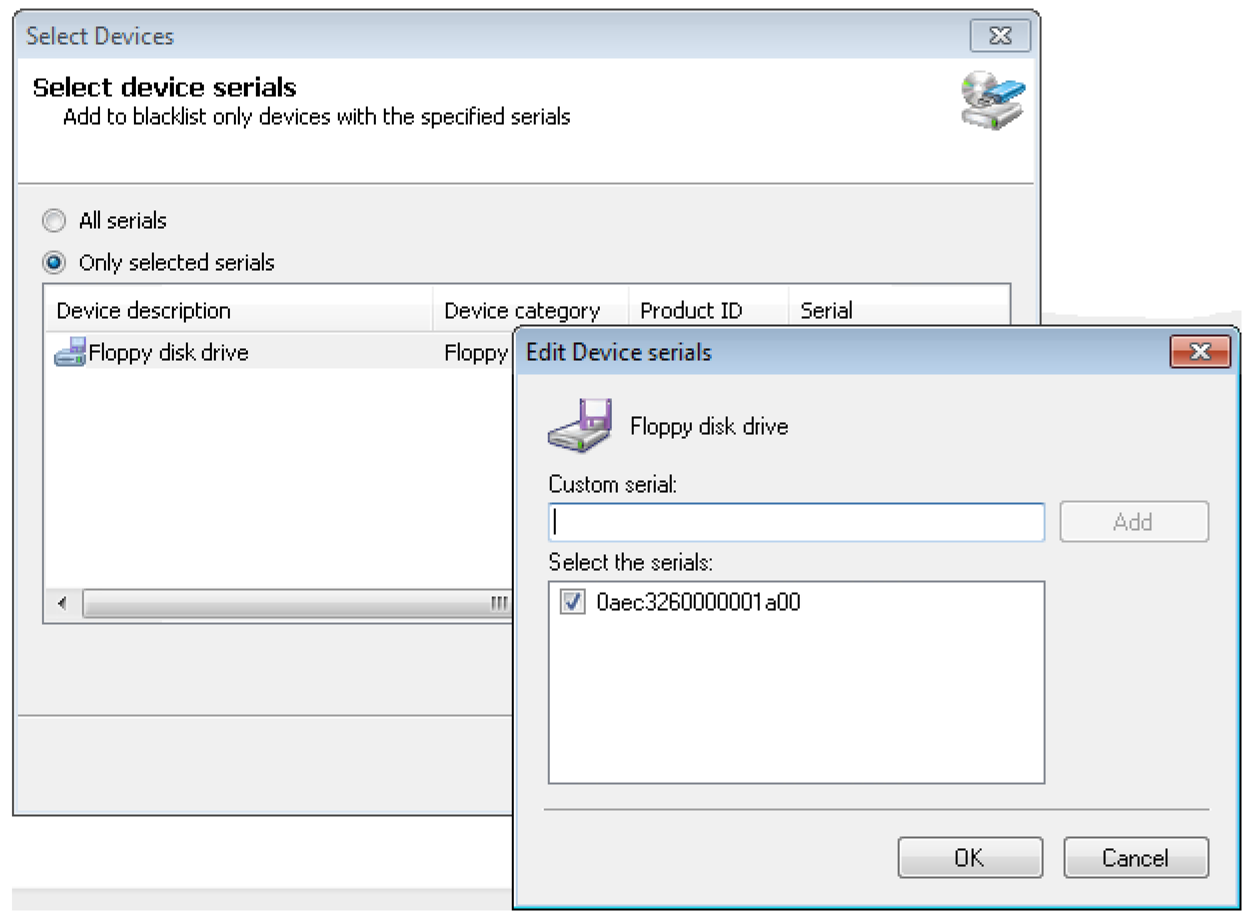
Si un dispositivo necesario no está incluido en la lista, haga clic en **Add New Device...** para especificar los detalles del dispositivo que desea agregar a la lista blanca y haga clic en **OK**.



Captura de pantalla 47: Opciones de selección de dispositivos: Select device serials

6. Seleccione la opción relacionada con los números de serie necesarios entre:

- **All serials:** Para incluir en la lista blanca todos los número de serie de un dispositivo específico. Haga clic en **Finish** y en **OK**.
- **Only selected serials:** Para especificar que solo los números de serie de un dispositivo en particular se deben agregar a la lista blanca. A continuación, resalte el dispositivo y haga clic en **Edit...** para seleccionar los números de serie para incluir en la lista blanca. Haga clic en **OK**, en **Finish** y en **OK**.



Captura de pantalla 48: Opciones de selección de dispositivos: Edit Device serials

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Deploy to all computers…**.

6.11 Configuración de privilegios de acceso temporal

GFI EndPointSecurity le permite otorgar acceso temporal a los usuarios. Esto les permite acceder a los dispositivos y puertos de conexión de equipos de destino protegidos durante una duración o un plazo determinados. Puede hacer esto directiva por directiva.

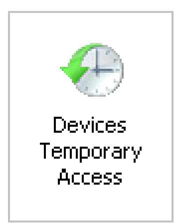
Cuando se otorga acceso temporal, se ignoran temporalmente los permisos y parámetros (por ej., filtros por tipo de archivo) establecidos en la directiva de protección aplicable para el equipo de destino.

Para obtener más información, consulte Cómo funciona GFI EndPointSecurity: Acceso temporal (página 18).

- Solicitud de acceso temporal a un equipo protegido
- Concesión de acceso temporal a un equipo protegido

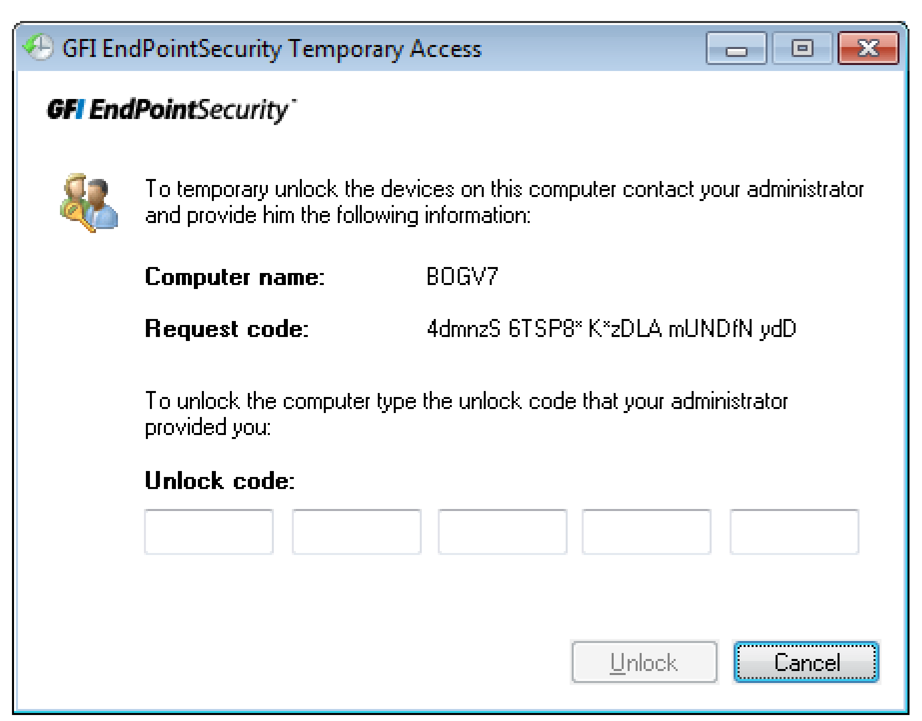
6.11.1 Solicitud de acceso temporal para un equipo protegido

Para generar un código de solicitud: herramienta:



Captura de pantalla 49: Icono Devices Temporary Access

1. En **Control Panel**, haga clic en **Devices Temporary Access**.



Captura de pantalla 50: GFI EndPointSecurityHerramienta Temporary Access

2. En el cuadro de diálogo **GFI EndPointSecurity Temporary Access**, tome nota del **código de solicitud** generado. Comuníquele los siguientes detalles al administrador de seguridad:

- Código de solicitud
- Tipo de puerto de dispositivo/conexión
- Cuándo requiere acceso
- Durante cuánto tiempo requiere acceso.

Mantenga abierta la herramienta GFI EndPointSecurity Temporary Access.

3. Cuando el administrador envíe el código de desbloqueo, escríbalo en el campo **Unlock code**.



Nota

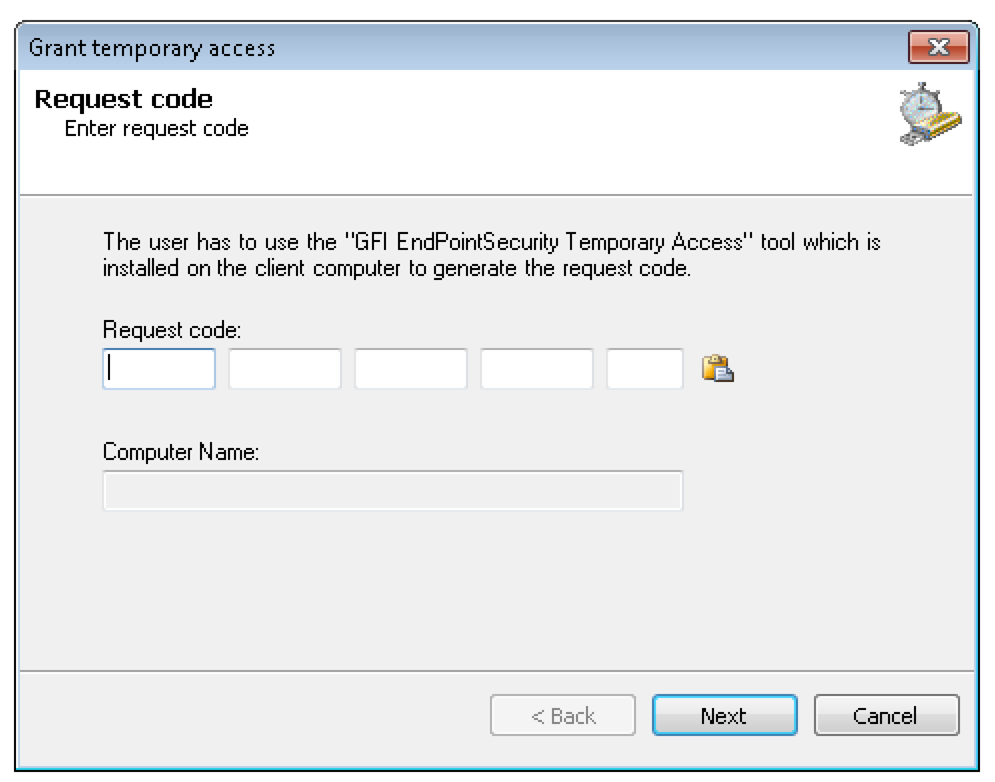
Un código de desbloqueo escrito en el equipo de destino protegido fuera del período de validez especificado no activará el acceso temporal.

4. Haga clic en **Unlock** para activar el acceso temporal. Ahora podrá acceder al dispositivo o puerto de conexión necesario.

6.11.2 Concesión de acceso temporal a un equipo protegido

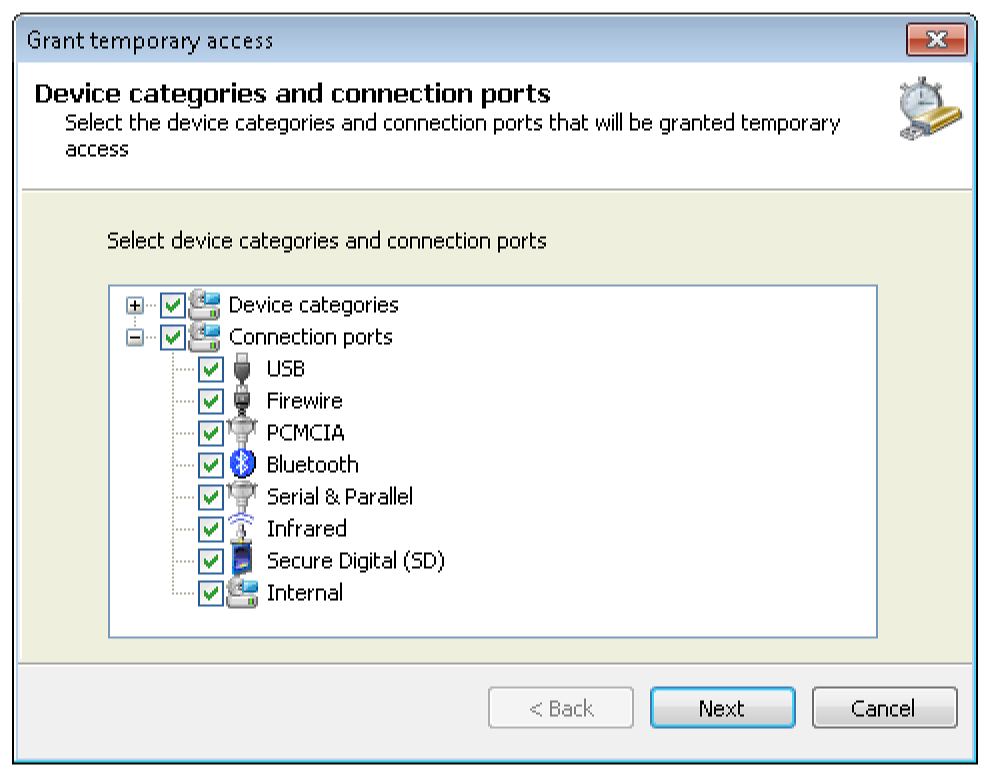
Para otorgar acceso temporal:

1. En la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Configuration** subficha > **Protection Policies.**
2. En el panel izquierdo, seleccione la directiva de protección que incluya el equipo en el que se deba conceder acceso temporal.
3. En la sección **Temporary Access** del panel derecho, haga clic en **Grant temporary access.**



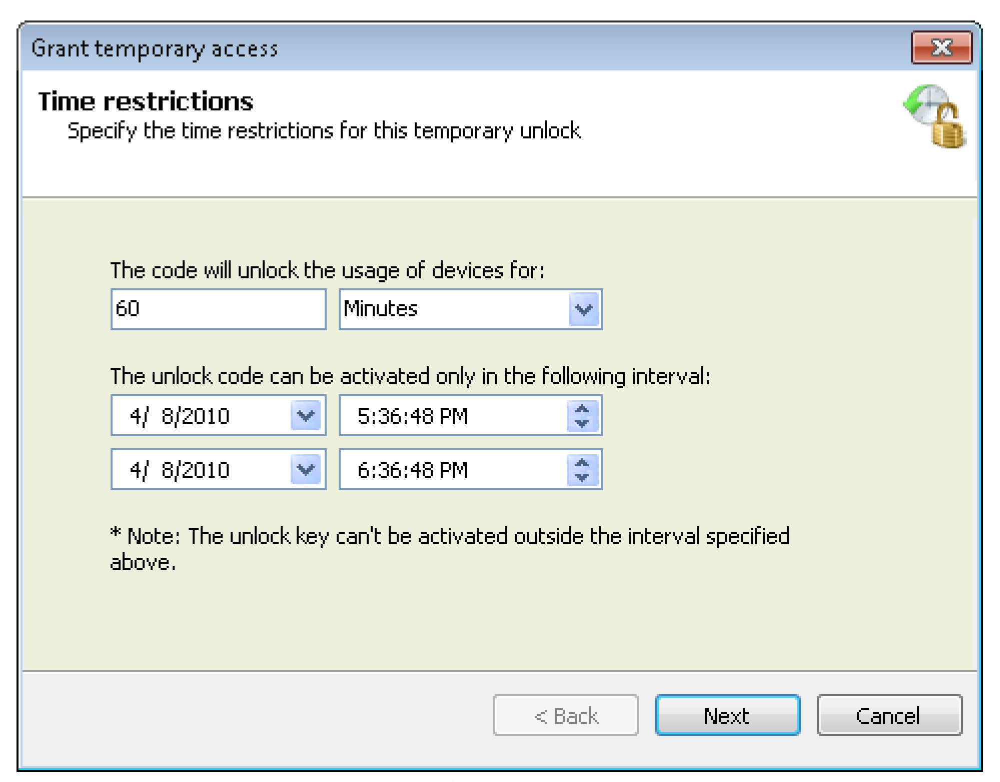
Captura de pantalla 51: Opciones de concesión de acceso temporal: Código de solicitud

4. En el cuadro de diálogo **Grant temporary access**, escriba el código de solicitud que recibió del usuario en el campo **Request code**. El nombre del equipo desde el cual se generó el código de solicitud se muestra en el campo **Computer Name**. Haga clic en **Next**.



Captura de pantalla 52: Opciones de concesión de acceso temporal: Categorías de dispositivo y puertos de conexión

5. Habilite las categorías de dispositivo o los puertos de conexión de la lista para los cuales otorgará acceso temporal y haga clic en **Next**.



Captura de pantalla 53: Opciones de concesión de acceso temporal: Restricciones de tiempo

6. Especifique la duración en la que se permite el acceso y el período de validez del código de desbloqueo; a continuación, haga clic en **Next**.

7. Tome nota del **código de desbloqueo** generado. Comuníquele el código al usuario que solicita acceso temporal y haga clic en **Finish**.

6.12 Configuración de filtros por tipo de archivo

GFI EndPointSecurity le permite especificar restricciones por tipo de archivo en los archivos, como .DOC o .XLS, que se copian en los archivos permitidos y desde ellos. Puede aplicar estas restricciones a usuarios o grupos de usuarios de Active Directory (AD). Puede hacer esto directiva por directiva.

El filtrado se basa en comprobaciones de extensión de archivo y comprobaciones de firma de tipo de archivo real. Las comprobaciones de firma de tipo de archivo real pueden realizarse en los siguientes tipos de archivo:

AVI	BMP	CAB	CHM	DLL	DOC	EMF	EXE	GIF	HLP
HTM	JPE	JPEG	JPG	LNK	M4A	MDB	MP3	MPEG	MPG
MSG	MSI	OCX	P7M	PDF	PPT	RAR	RTF	SCR	SYS
TIF	TIFF	TXT	URL	WAV	XLS	ZIP	DOCX	XLSX	PPTX



Nota 1

Con cualquier otro tipo de archivo no especificado anteriormente, el filtrado se basa únicamente en la extensión de archivo.

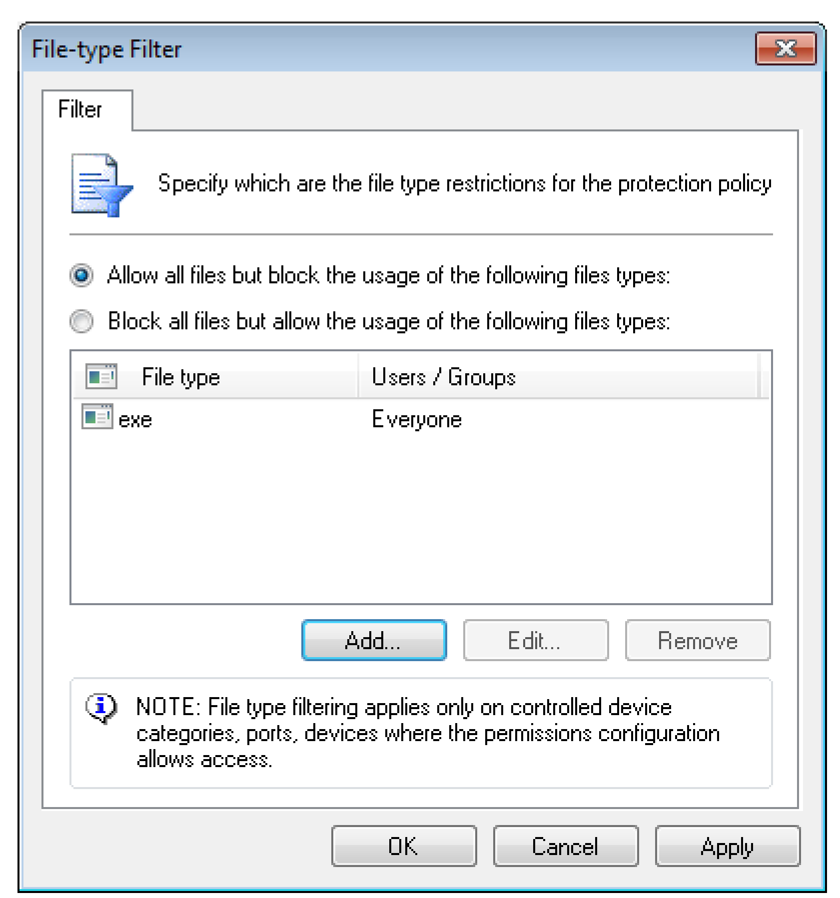


Nota 2

El filtro por tipo de archivo se aplica únicamente a las categorías de dispositivos o los puertos para los cuales se han establecido permisos para permitir el acceso.

Para configurar restricciones por tipo de archivo para los usuarios de una directiva de protección específica:

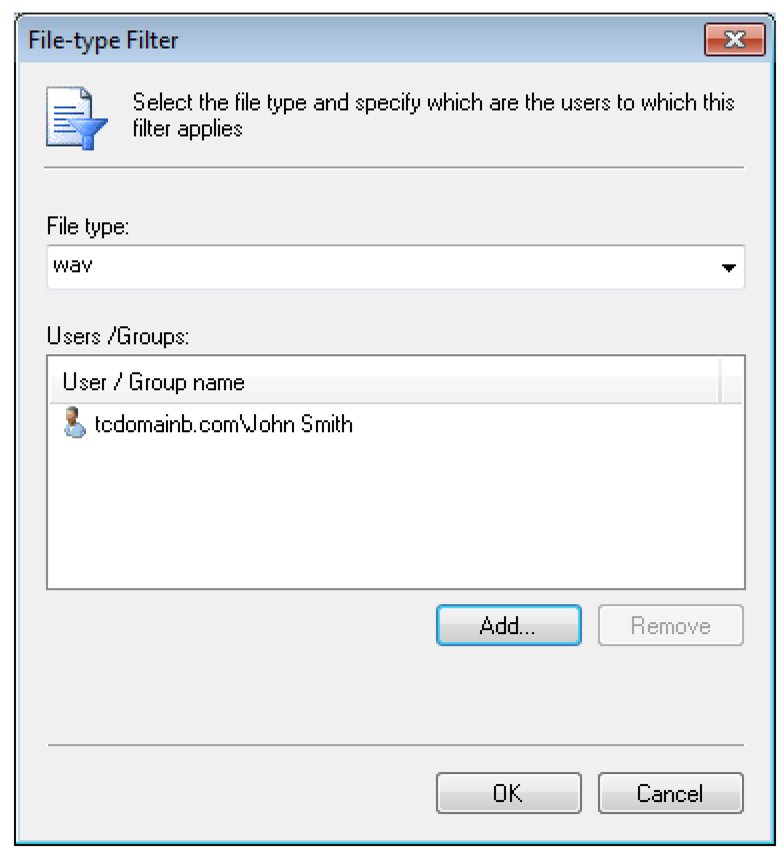
1. En la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Configuration > Protection Policies**.
2. En el panel izquierdo, seleccione la directiva de protección para la cual desea especificar restricciones por tipo de archivo.
3. En la sección **File control** del panel derecho, haga clic en **File-type Filter**.



Captura de pantalla 54: Opciones de filtro por tipo de archivo

4. En el cuadro de diálogo File-type Filter, seleccione la restricción que desee aplicar a esta directiva:

- Allow all files but block the usage of the following file types
- Block all files but allow the usage of the following file types



Captura de pantalla 55: Opciones de usuario y filtro por tipo de archivo

5. Haga clic en **Add…** y seleccione el tipo de archivo de la lista desplegable **File type** o escríbalo.
6. Haga clic en **Add…** para especificar los grupos de usuarios a los que se les permite o bloquea el acceso al tipo de archivo especificado y haga clic en **OK**. Repita los dos pasos secundarios anteriores para cada tipo de archivo que desee restringir.
7. Haga clic en **OK** dos veces.

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. En la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Configuration** > subficha **Computers**.
2. En la sección **Common tasks** del panel izquierdo, haga clic en **Deploy to all computers…**.

6.13 Configuración de reconocimiento de contenido

GFI EndPointSecurity le permite especificar las restricciones de contenido de los archivos para una directiva de protección en particular. La función de reconocimiento de contenido revisa los archivos y traduce los extremos a través de dispositivos extraíbles e identifica el contenido en función de expresiones regulares preconfiguradas y personalizadas y archivos de diccionario. De forma predeterminada, el módulo busca detalles confidenciales seguros como números de seguridad social y números de cuenta primarios, así como información relacionada con empresas y compañías como nombres de enfermedades, fármacos, productos químicos peligrosos y lenguaje trivial o términos étnicos/racistas.

- Puede configurar comprobaciones de contenido como una directiva global de manera similar al módulo de comprobación de archivos.

6.13.1 Administración de opciones de reconocimiento de contenido

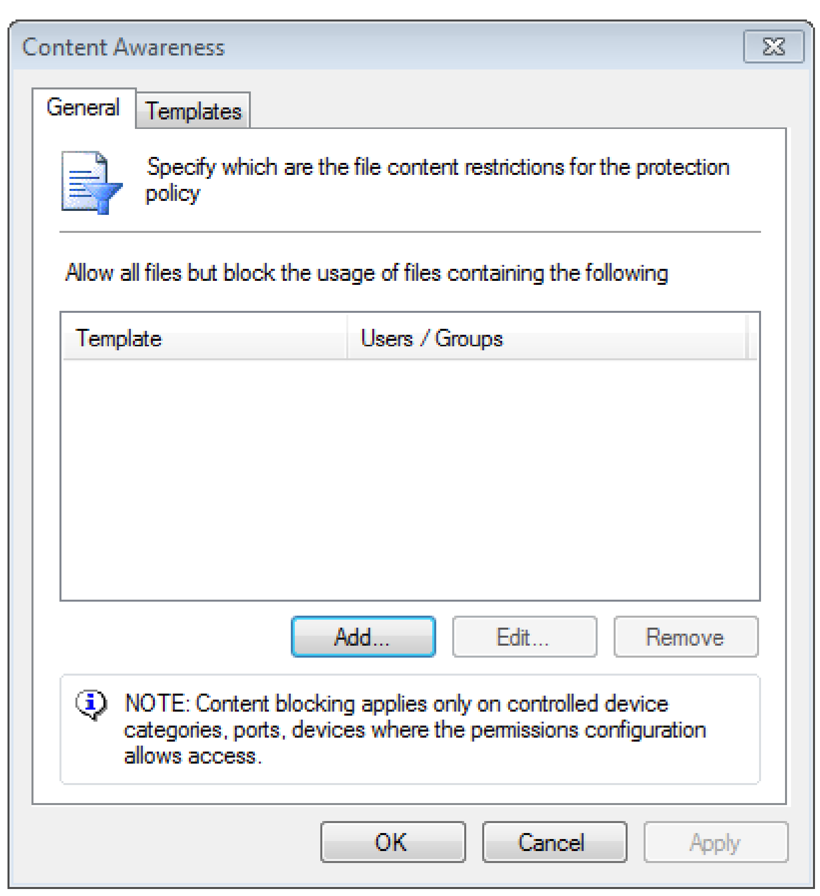
Para configurar opciones de reconocimiento de contenido para los usuarios

en una directiva de protección específica:

1. En la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Configuration > Protection Policies**.

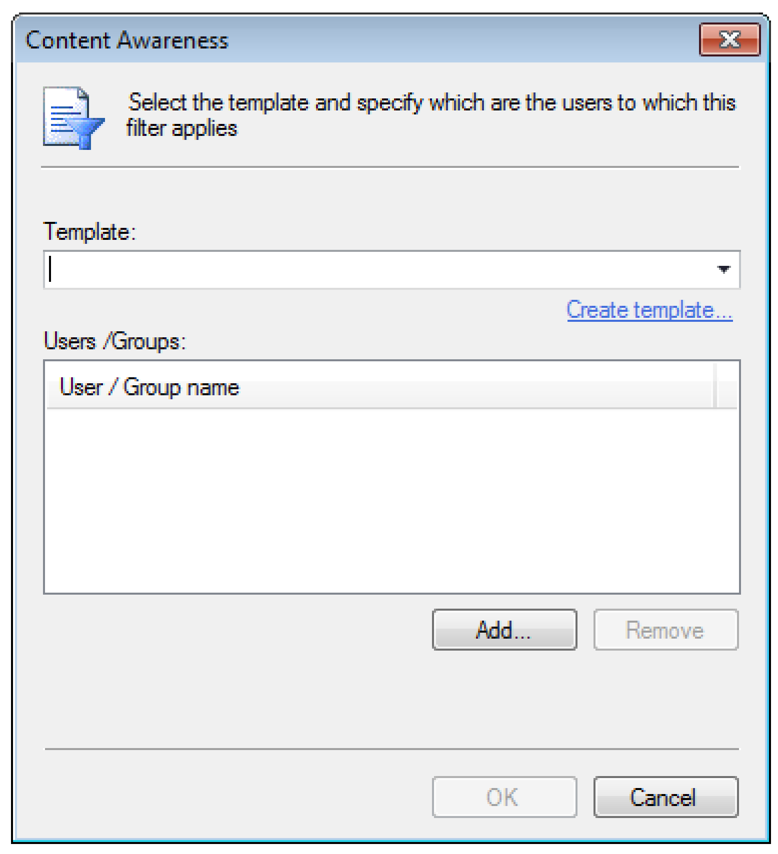
2. En el panel izquierdo, seleccione la directiva de protección para la cual desea especificar restricciones de contenido.

3. En la sección **File control** del panel derecho, haga clic en **Content awareness**.



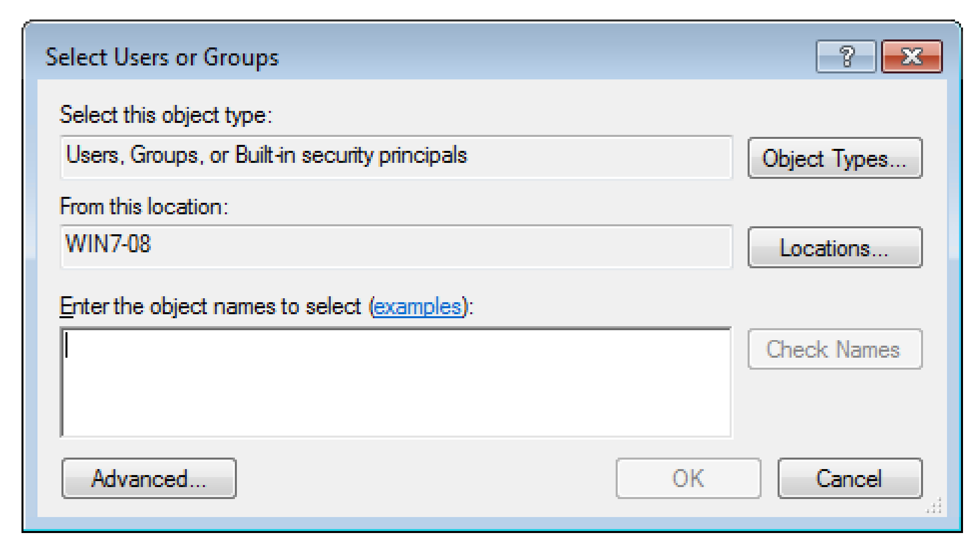
Captura de pantalla 56: Opciones de reconocimiento de contenido

4. En el cuadro de diálogo Content awareness, haga clic en **Add** para seleccionar la plantilla que desee aplicar a esta directiva:



Captura de pantalla 57: Agregar una plantilla nueva

5. Haga clic en **Add...** y seleccione la plantilla de la lista desplegable **Template** o escríbala.
6. Haga clic en **Add...** para especificar los grupos de usuarios y haga clic en **OK**. Repita los dos pasos secundarios anteriores para cada plantilla que se aplicará.
7. Haga clic en **OK**.

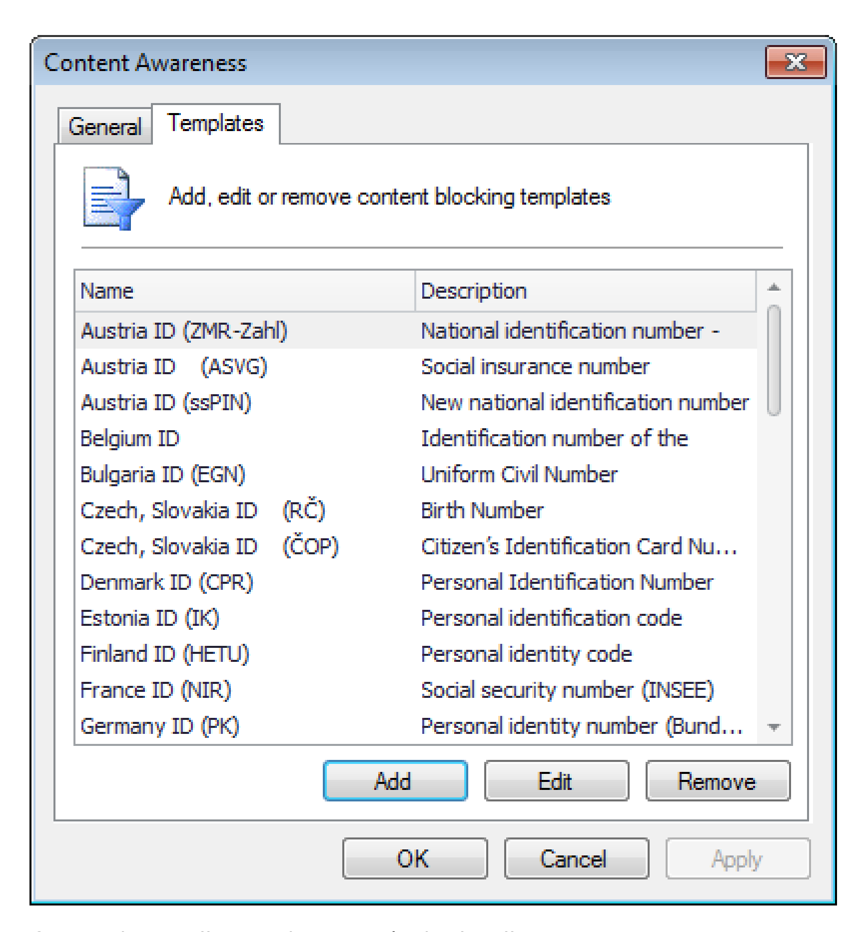


Captura de pantalla 58: Selección de usuarios o grupos

6.13.2 Administración de opciones de plantillas

Para agregar, editar o quitar plantillas predefinidas:

1. Haga clic en **Templates** y seleccione una plantilla de la lista **Template**.
2. Haga clic en **Add**, **Edit** o **Remove** para modificar o eliminar las plantillas.

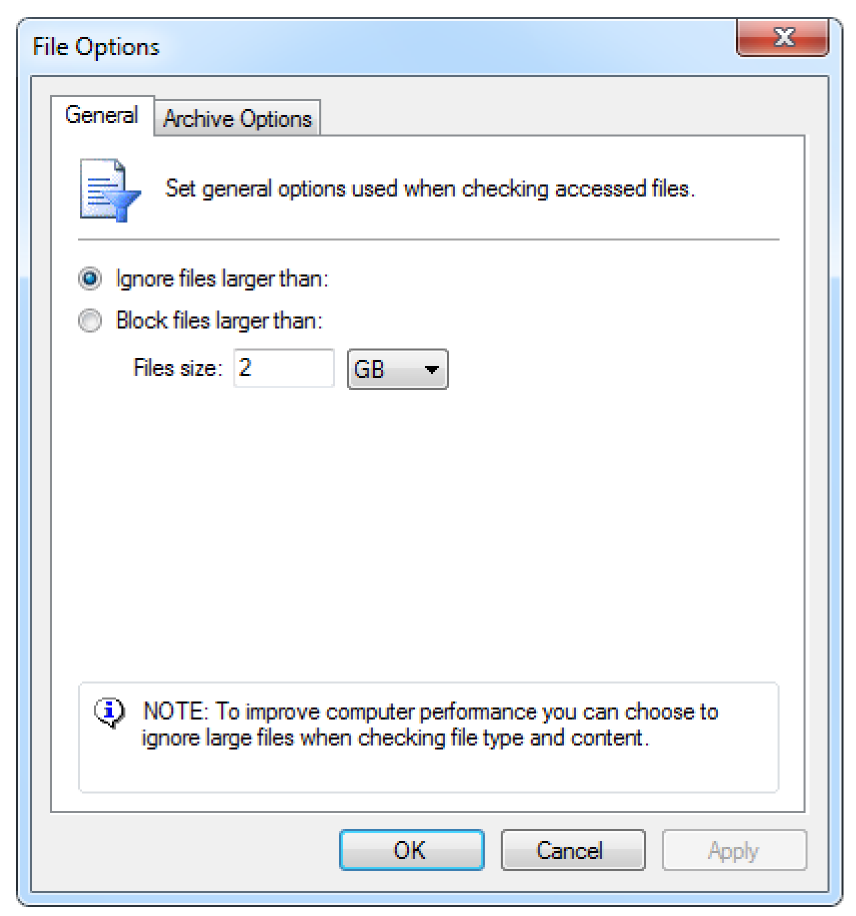


Captura de pantalla 59: Administración de plantillas

6.14 Configuración de opciones de archivo

GFI EndPointSecurity le permite especificar las opciones necesarias para bloquear o permitir archivos en función del tamaño. GFI EndPointSecurity también le permite ignorar archivos de gran tamaño al comprobar el tipo de archivo, el contenido y los archivos almacenados.

1. En la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Configuration > Protection Policies**.
2. En el panel izquierdo, seleccione la directiva de protección para la cual desea especificar restricciones de opciones de archivo.
3. En la sección **File control** del panel derecho, haga clic en **File options**.

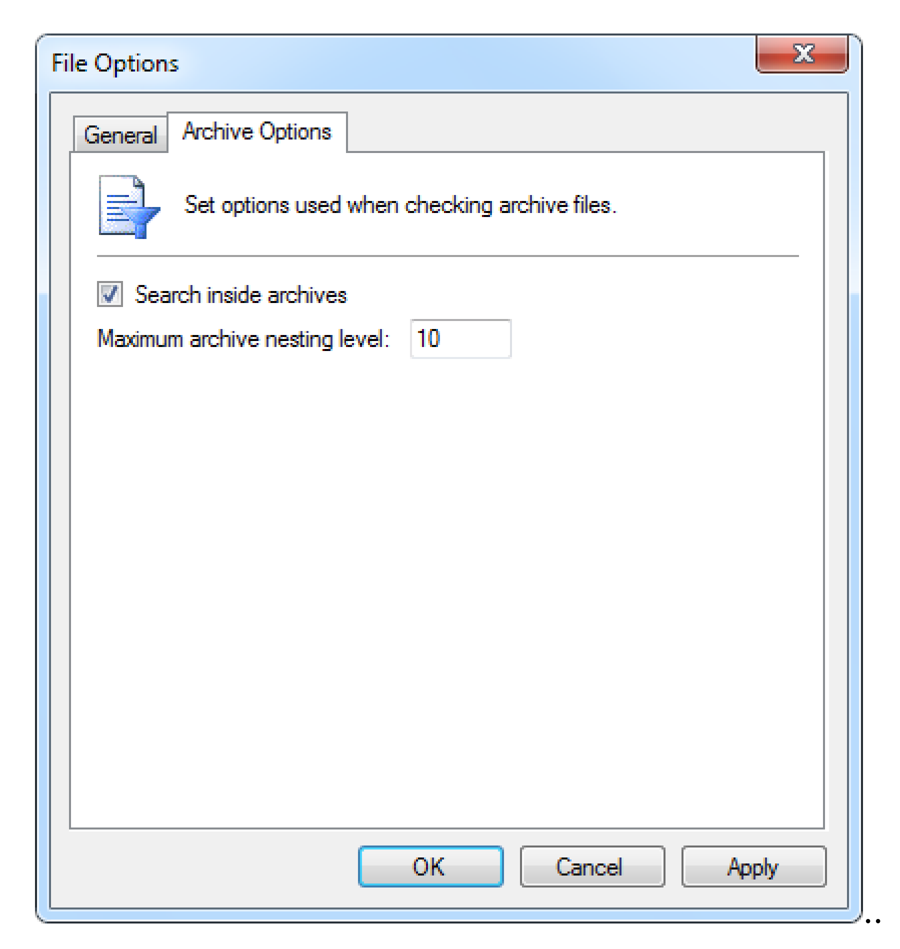


Captura de pantalla 60: Opciones de archivo

4. En el cuadro de diálogo File options, seleccione entre las siguientes opciones:

Tabla 13: Opciones de archivo: Opciones de usuario

Opción	Descripción
Ignore files larger than:	Se ignoran los archivos con un tamaño superior al especificado al comprobar los archivos a los que se accedió.
Block files larger than:	Se bloquean los archivos con un tamaño superior al especificado al comprobar los archivos a los que se accedió.



Captura de pantalla 61: Opciones de usuario y filtro por tipo de archivo

5. En la ficha **Archive Options**, habilite o deshabilite **Search inside archives** y especifique el nivel de anidado de archivo que desee usar al comprobar los archivos almacenados.

6. Haga clic en **OK**.

6.15 Configuración de cifrado de seguridad

GFI EndPointSecurity le permite configurar los parámetros que se adaptan específicamente a los dispositivos cifrados. También le permite cifrar dispositivos que todavía no están asegurados.

- Configuración de dispositivos con Microsoft BitLocker To Go
- Configuración de cifrado de volúmenes

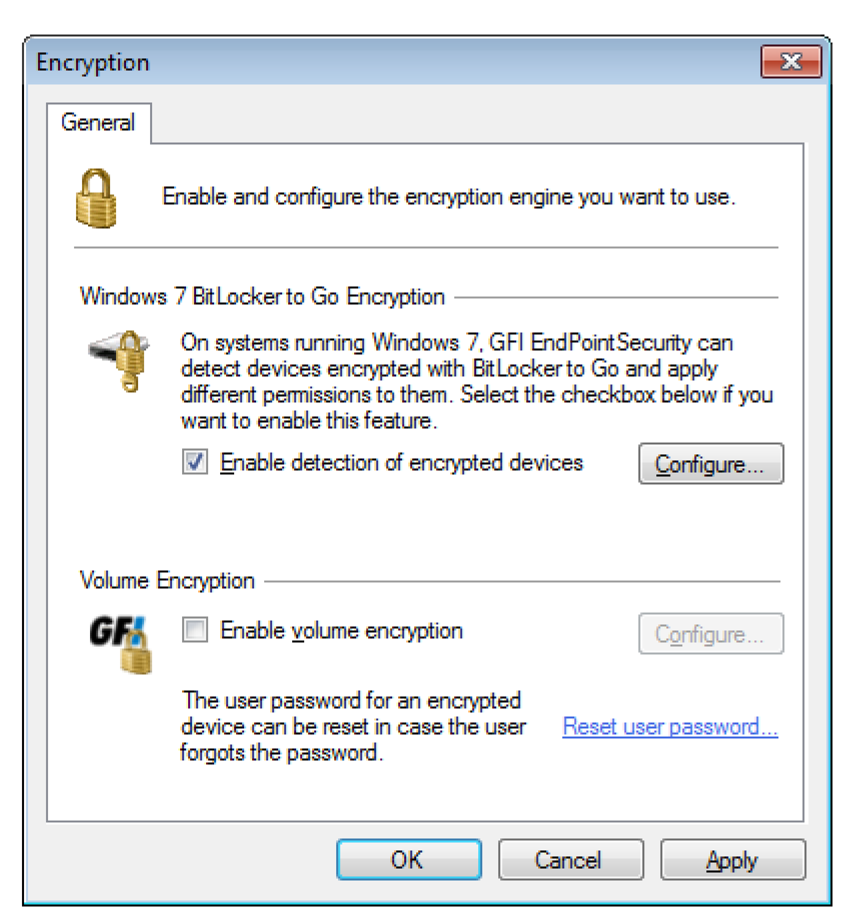
6.15.1 Configuración de dispositivos con Microsoft BitLocker To Go

GFI EndPointSecurity puede detectar dispositivos de almacenamiento cifrados con Microsoft BitLocker To Go. Esto le permite configurar diferentes permisos en cada dispositivo. Para habilitar la detección de Microsoft BitLocker To Go:

1. En la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Configuration > Protection Policies**.

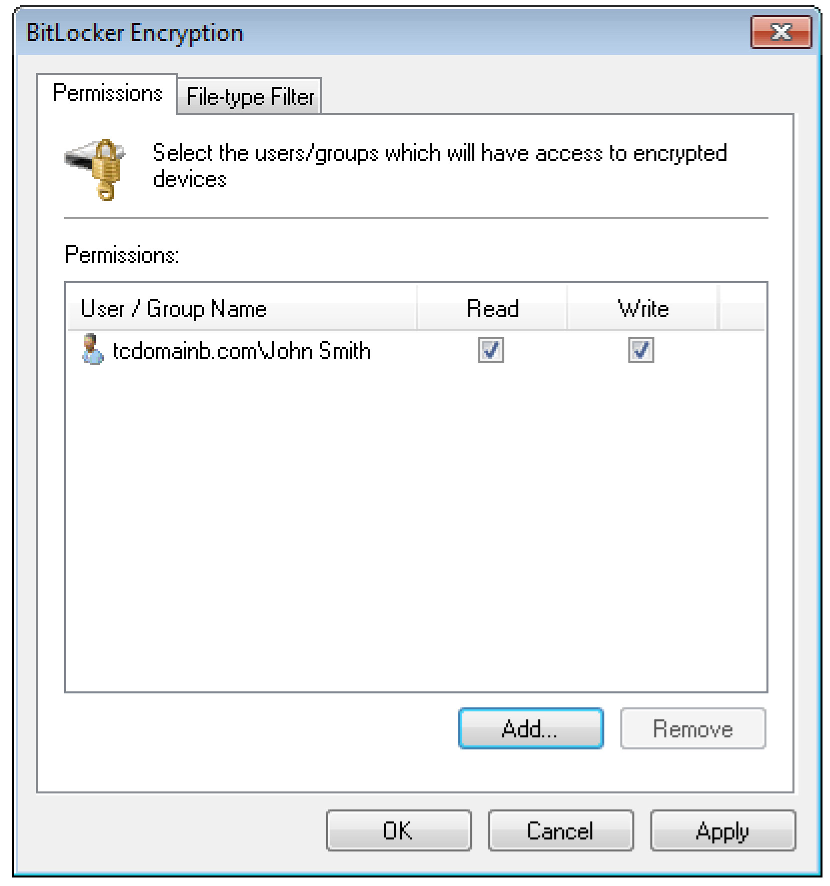
2. En el panel izquierdo, seleccione la directiva de protección para la cual desea aplicar la directiva de cifrado.

3. En la sección **Security** del panel derecho, haga clic en **Encryption**.



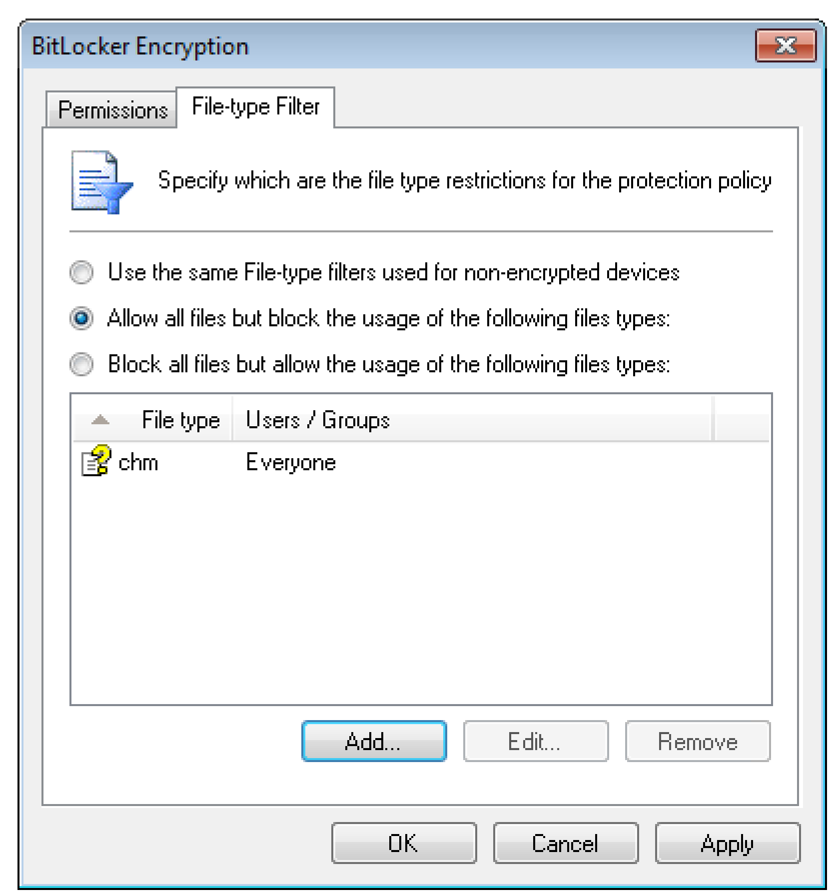
Captura de pantalla 62: Opciones de cifrado: Ficha General

4. Seleccione **Enable detection of encrypted devices** y haga clic en **Configure...**



Captura de pantalla 63: Opciones de cifrado: Ficha Permissions

5. Haga clic en **Add...** para especificar los usuarios y grupos con acceso a dispositivos cifrados.



Captura de pantalla 64: Opciones de cifrado: Ficha File-type Filter

6. Seleccione la ficha **File-type Filter** para configurar los tipos de archivo que desee restringir.
7. Seleccione la restricción que desee aplicar a esta directiva:

- Use the same File-type filters used for non-encrypted devices
- Allow all files but block the usage of the following file types
- Block all files but allow the usage of the following file types

8. Utilice los botones **Add**, **Edit** y **Remove** para administrar los tipos de archivo.
9. Haga clic en **OK**.

6.15.2 Configuración de cifrado de volúmenes

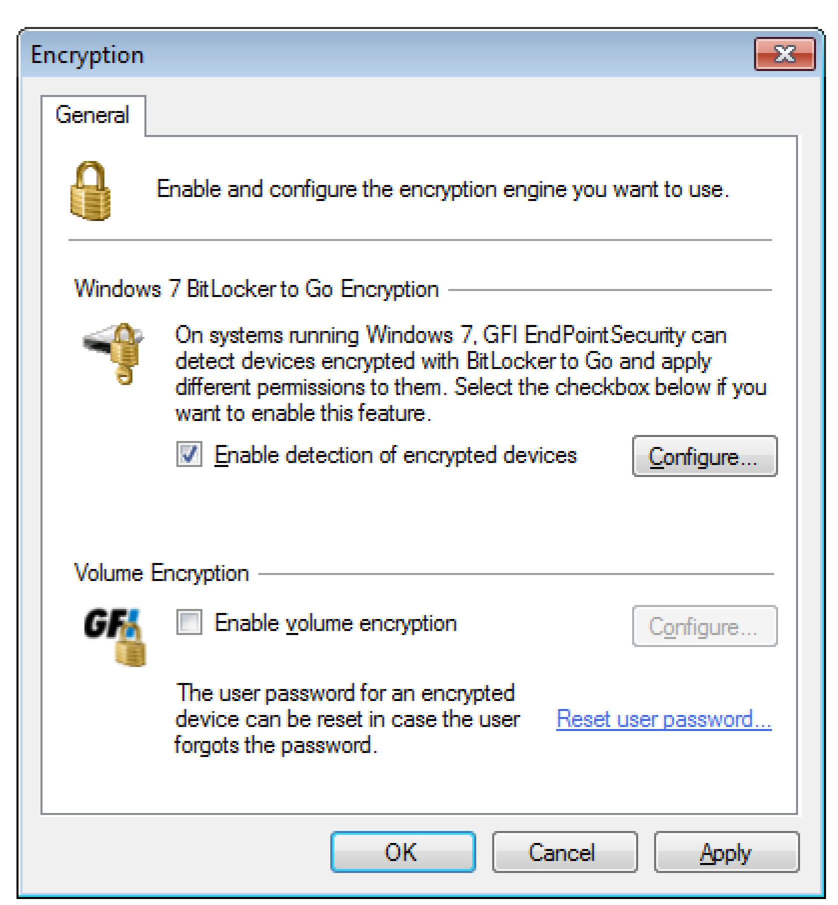
El cifrado de volúmenes le permite cifrar el contenido de los dispositivos USB mediante cifrado AES 256. Cuando se fuerza el cifrado de volúmenes, los usuarios deben proporcionar una contraseña para cifrar los datos de los dispositivos de almacenamiento o para acceder a ellos. Para forzar el cifrado de volúmenes en agentes instalados:



Nota

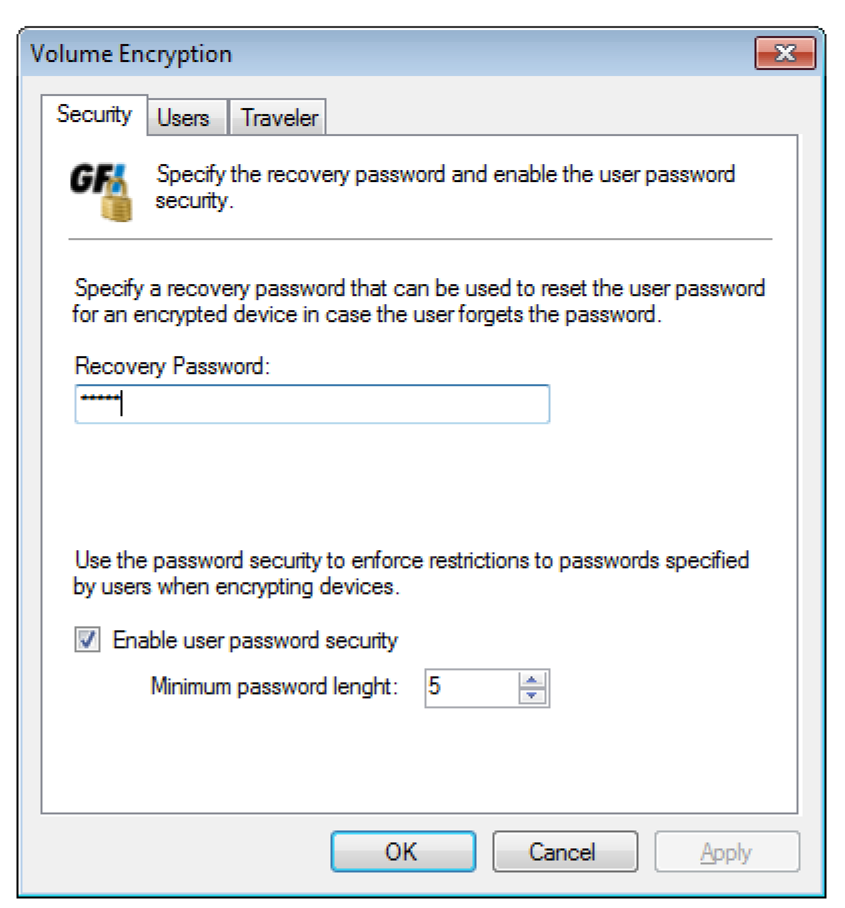
El cifrado a petición es posible incluso si no lo fuerza el administrador sino directamente el usuario final al hacer clic en la entrada **Encrypt...** del menú contextual de shell de una unidad extraíble.

1. En la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Configuration > Protection Policies**.
2. En el panel izquierdo, seleccione la directiva de protección para la cual desea aplicar la directiva de cifrado.
3. En la sección **Security** del panel derecho, haga clic en **Encryption**.



Captura de pantalla 65: Opciones de cifrado: Ficha General

4. Seleccione **Enable volume encryption**. Haga clic en **Configure**. Haga clic en **Reset user password** para restablecer la contraseña de cifrado de un usuario específico.

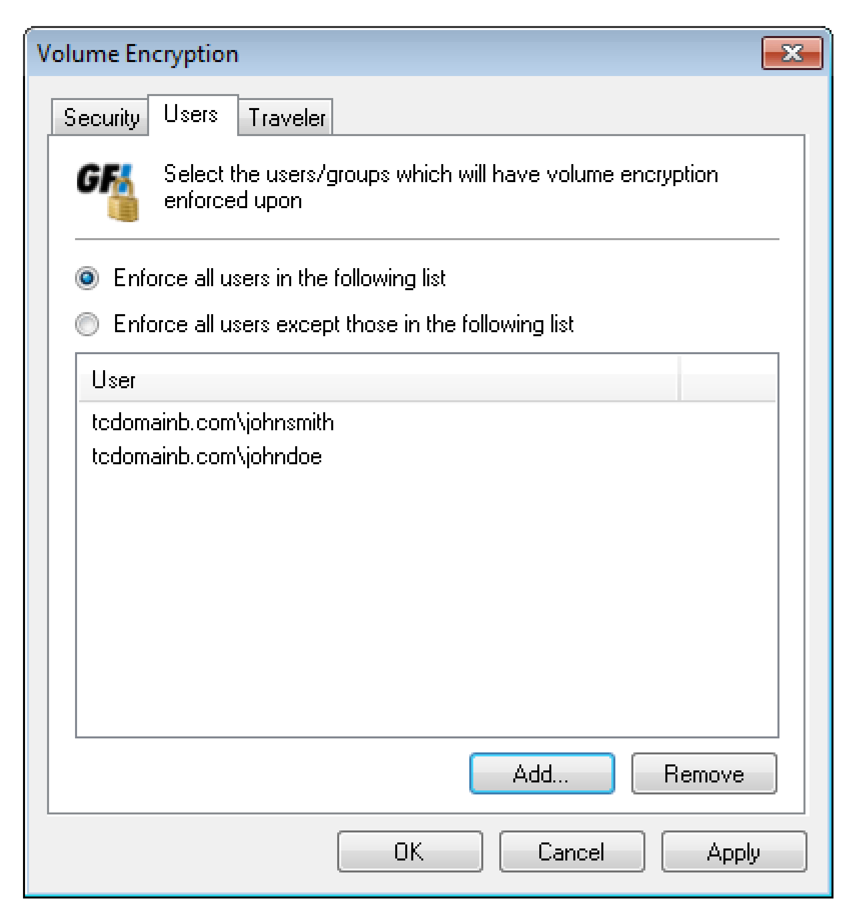


Captura de pantalla 66: Opciones de cifrado: Ficha Security

5. En la ficha **Security**, configure las funciones que se describen a continuación:

Tabla 14: Cifrado de volúmenes: Opciones de seguridad

Opción	Descripción
Recovery Password	La clave de una contraseña utilizada si los usuarios olvidan o pierden sus contraseñas.
Enable user password security	Fuerza las restricciones de las contraseñas especificadas por los usuarios finales. En **Minimum password length**, especifique la longitud de contraseña mínima aceptable.

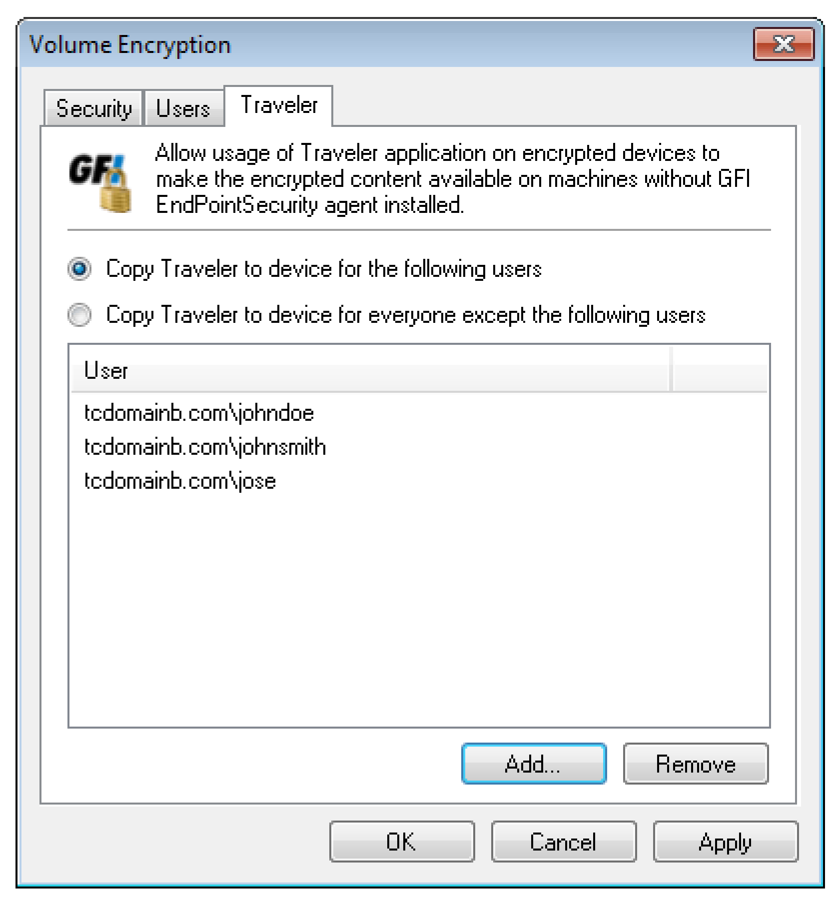


Captura de pantalla 67: Opciones de cifrado: Ficha Users

6. Seleccione la ficha **Users** y configure las siguientes opciones:

Tabla 15: Cifrado de volúmenes: Opciones de usuario

Opción	Descripción
Enforce all users in the following list	Seleccione los usuarios que tendrán el cifrado de volúmenes forzado en sus dispositivos portátiles. Use los botones **Add** y **Remove** para administrar los usuarios seleccionados.
Enforce all users except those in the following list	Seleccione los usuarios que estarán exentos del cifrado de volúmenes. Use los botones Add y Remove para administrar los usuarios seleccionados.



Captura de pantalla 68: Opciones de cifrado: Ficha Traveler



Nota

Traveler es una aplicación que se puede instalar automáticamente en los dispositivos de almacenamiento a través de GFI EndPointSecurity. Esta aplicación le permite descifrar los datos cifrados por GFI EndPointSecurity en dispositivos de almacenamiento, desde equipos que no estén ejecutando un agente de GFI EndPointSecurity.

7. Seleccione la ficha **Traveler** y configure las siguientes opciones:

Tabla 16: Cifrado de volúmenes: Opciones de desplazamiento

Opción	Descripción
Copy Traveler to device for the following users	Seleccione los usuarios que tendrán Traveler instalado en sus equipos. Use los botones **Add** y **Remove** para administrar los usuarios seleccionados.
Copy Traveler to device for eve-ryone except the following users	Seleccione los usuarios que estarán exentos de la instalación de Traveler. Use los botones **Add** y **Remove** para administrar los usuarios seleccionados.

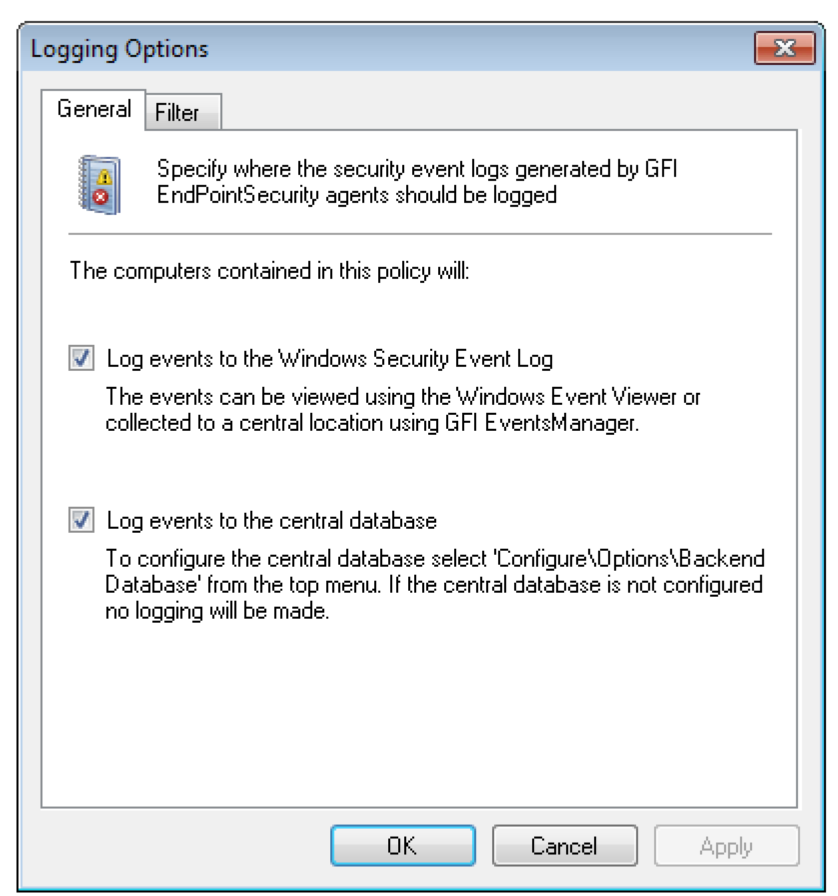
8. Haga clic en **Apply** y en **OK**.

6.16 Configuración del registro de eventos

Los agentes de GFI EndPointSecurity registran eventos relacionados con los intentos realizados para acceder a dispositivos y a puertos de conexión en los equipos de destino. Además, los agentes registran los eventos relacionados con operaciones de servicio. Puede especificar dónde se deben almacenar estos eventos, así como qué tipos de eventos se deben registrar. Puede hacer esto directiva por directiva.

Para especificar opciones de registro para los usuarios de una directiva de protección:

1. Haga clic en la ficha **Configuration** > **Protection Policies**.
2. En **Protection Policies** > **Security**, seleccione la directiva de protección que desee configurar.
3. En la sección **Logging and Alerting** del panel derecho, haga clic en **Set Logging Options**.

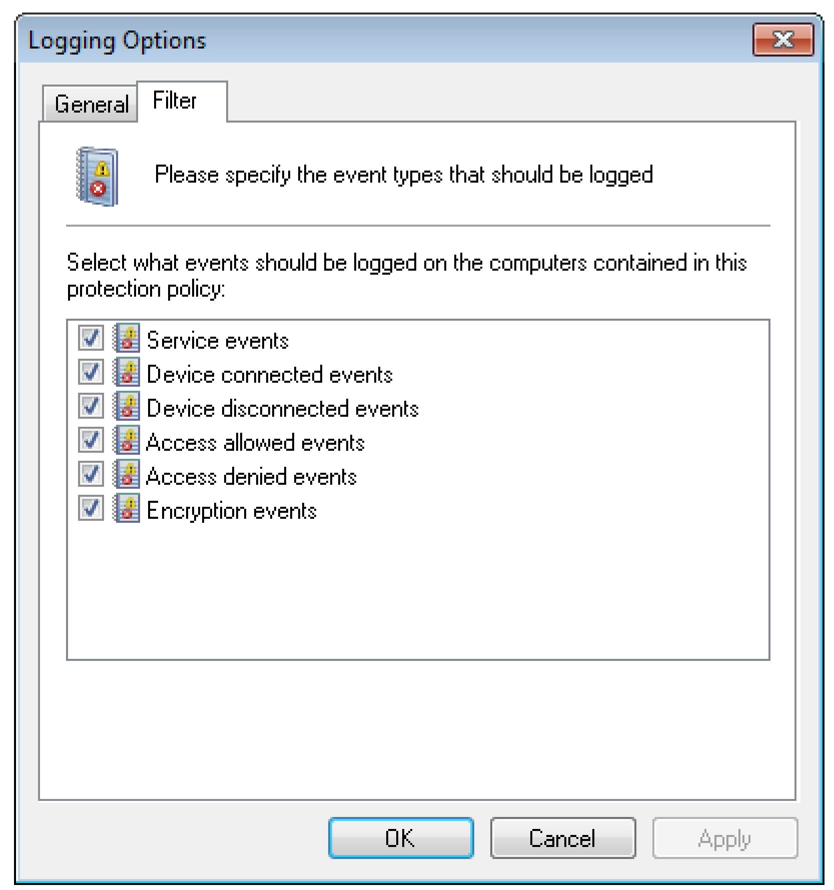


Captura de pantalla 69: Opciones de registro: Ficha General

4. En el cuadro de diálogo **Logging Options**, haga clic en la ficha **General**.
5. Habilite o deshabilite las ubicaciones donde se almacenarán los eventos generados por esta directiva de protección:

Opción	Descripción
Log events to the Windows Security Event Log	Puede ver los eventos a través del Visor de eventos de Windows de cada equipo de destino o a través de GFI EventsManager después de que se recopilan en una ubicación central.
Log events to the central database	Puede ver los eventos dentro de la subficha **Logs Browser** en la consola de administración de GFI EndPointSecurity. Esta opción requiere la configuración de una base de datos central. Para obtener más información, consulte Administración del back-end de base de datos (página 128).

Si ambas opciones están habilitadas, se registran los mismos datos en ambas ubicaciones.



Captura de pantalla 70: Opciones de registro: Ficha Filter

6. Seleccione la ficha **Filter** y elija cualquiera de los siguientes tipos de eventos para registrar a través de esta directiva de protección. Haga clic en **OK**.

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Deploy to all computers…**.

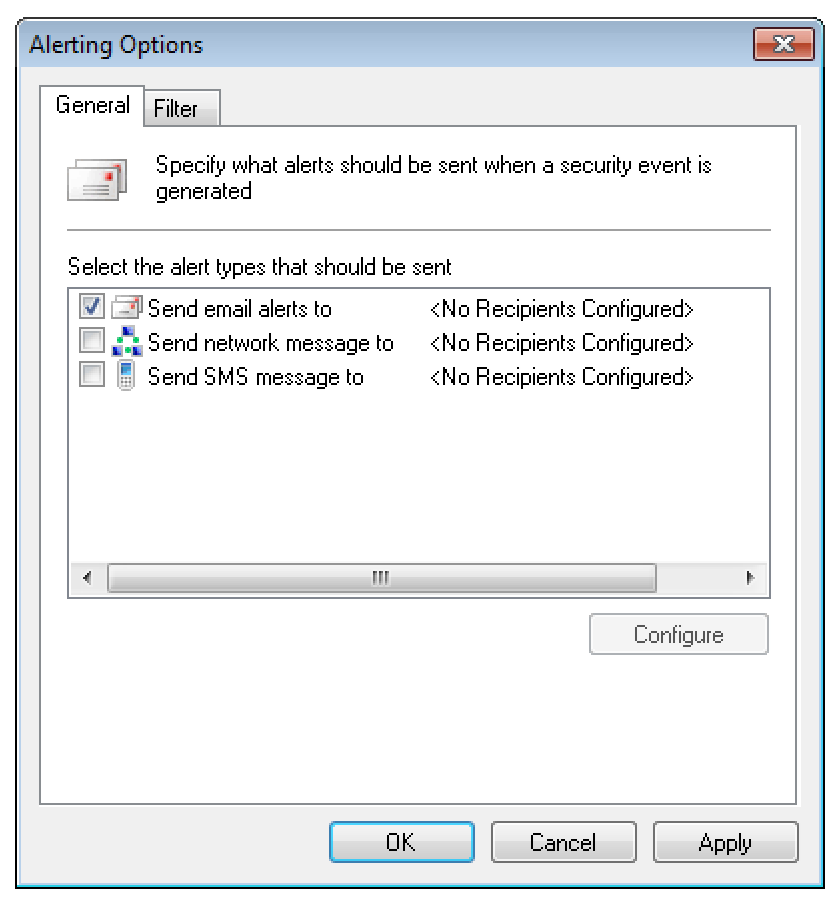
6.17 Configuración de alertas

GFI EndPointSecurity puede configurarse para enviar alertas a destinatarios específicos cuando se generan eventos particulares. Puede configurar las alertas para que se envíen a través de varias opciones de alerta, así como también especificar los tipos de eventos para los cuales se envían las alertas. Puede hacer esto directiva por directiva.

Los destinatarios de alertas no son usuarios o grupos de usuarios de Active Directory (AD), sino que son cuentas de perfil creadas por GFI EndPointSecurity para contener los detalles de contacto de los usuarios a los que se destinan las alertas. Es mejor crear los destinatarios de las alertas antes de configurar las alertas. Para obtener más información, consulte Configuración de destinatarios de alertas (página 138).

Para especificar opciones de alerta para los usuarios de una directiva de protección:

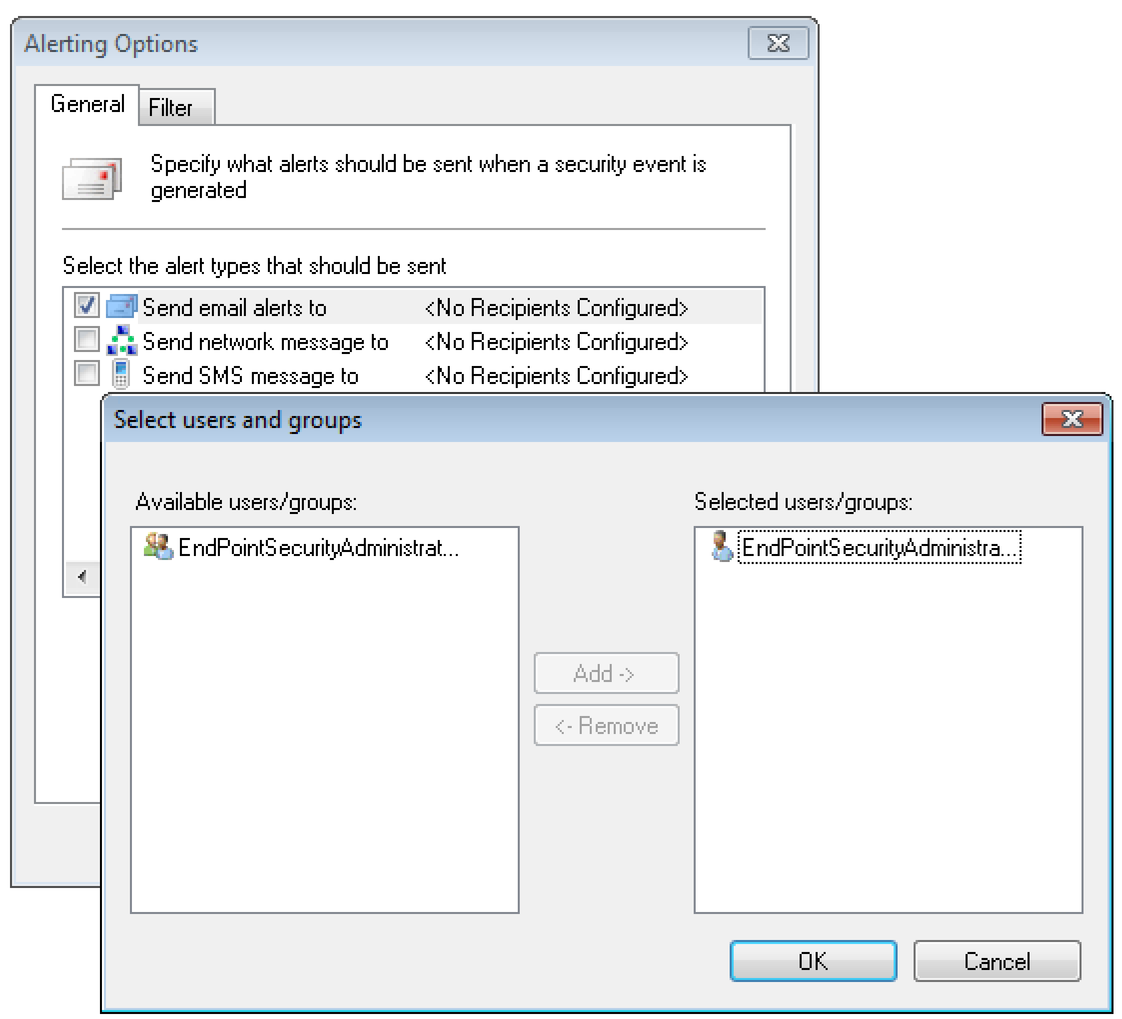
1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. En la sección **Logging and Alerting** del panel derecho, haga clic en **Alerting options**.



Captura de pantalla 71: Opciones de alerta: Ficha General

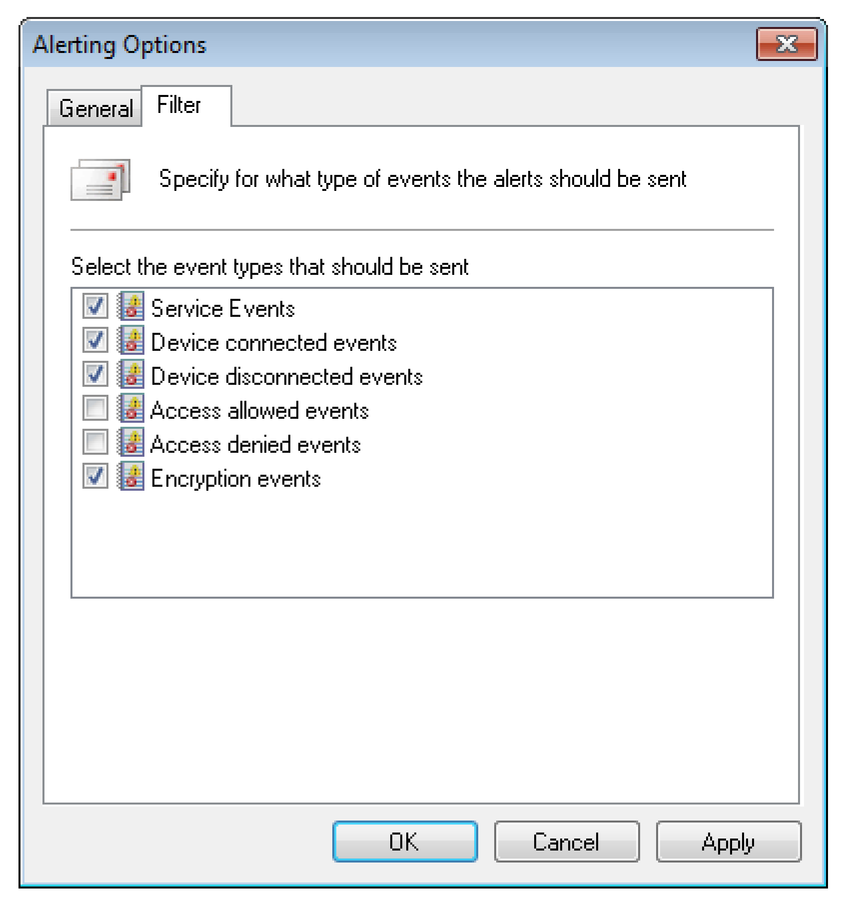
4. En el cuadro de diálogo **Alerting Options**, haga clic en la ficha **General** y seleccione cualquiera de los siguientes tipos de alerta para enviar:

- Alertas de correo electrónico
- Mensajes de red
- Mensajes SMS.



Captura de pantalla 72: Opciones de alerta: Configuración de usuarios y grupos

5. Para cada tipo de alerta habilitado, resáltelo y haga clic en **Configure** para especificar destinatarios de alertas. Haga clic en **OK**.



Captura de pantalla 73: Opciones de alerta: Ficha Filter

6. Seleccione la ficha **Filter** y elija cualquiera de los siguientes tipos de eventos para los cuales la directiva de protección envía las alertas. Haga clic en **OK**.

Para implementar actualizaciones de la directiva de protección en los equipos de destino especificados en la directiva:

1. Haga clic en la ficha **Configuration** > **Computers**.
2. En **Common tasks**, haga clic en **Deploy to all computers…**.

6.18 Configuración de una directiva como predeterminada

GFI EndPointSecurity le proporciona la facilidad de definir la directiva de protección asignada a equipos de red recientemente detectados por la función de implementación de agente. Puede hacer esto directiva por directiva.

De forma predeterminada, la función de implementación de agente está establecida para usar la directiva de protección de **control general**, pero puede elegir otra directiva de protección como predeterminada.

Para elegir otra directiva de protección como predeterminada:

1. Haga clic en la ficha **Configuration > Protection Policies**.
2. En **Protection Policies > Security**, seleccione la directiva de protección que desee configurar.
3. En la sección **Common tasks** del panel izquierdo, haga clic en **Set as default policy**.

7 Detección de dispositivos

GFI EndPointSecurity le permite consultar de manera rápida y transparente extremos de red organizativos, para ubicar e informar todos los dispositivos que están o han estado conectados a los equipos de destino examinados. La aplicación identifica de manera granular los dispositivos de extremo conectados a los equipos de destino, actual e históricamente, y muestra la información detallada en pantalla cuando se completa el examen.

Use la ficha **Scanning** para examinar equipos de destino y detectar dispositivos conectados. De forma predeterminada, GFI EndPointSecurity examina todas las categorías de dispositivo y los puertos de conectividad admitidos.

Un equipo de destino detectado puede ser cualquier equipo de la red, y puede no estar incluido en ninguna directiva de protección de GFI EndPointSecurity. El examen de dispositivos debe ejecutarse en una cuenta que tenga privilegios administrativos en los equipos de destino.

Temas de este capítulo

7.1 Ejecución de un examen de dispositivos

La ejecución de un examen de dispositivos es fundamental para detectar dispositivos nuevos. GFI EndPointSecurity le permite buscar dispositivos nuevos conectados al equipo de destino. Esto le permite agregar dispositivos nuevos en cuanto se detecten.



Nota:

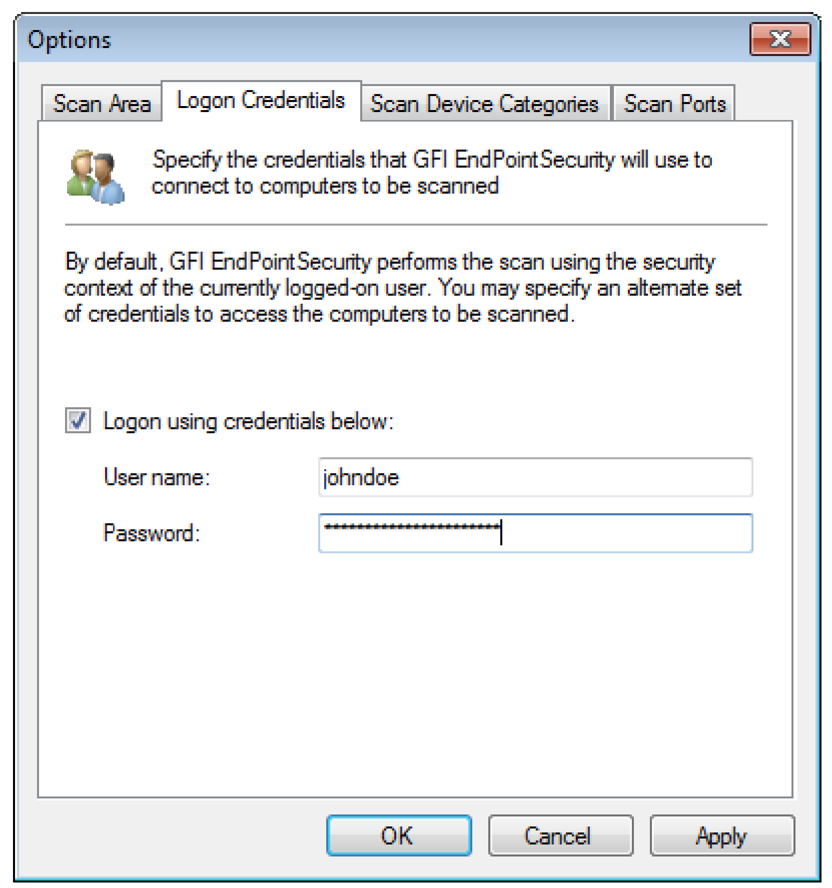
En Microsoft Vista, Microsoft Windows 7 y Microsoft Windows 2008 se incorporó una nueva directiva de seguridad que debe habilitarse para que el detector de dispositivos de GFI EndPointSecurity enumere los dispositivos físicos ubicados en el equipo.

Para habilitar el acceso remoto a la interfaz Plug and Play:

1. Inicie sesión en el equipo con Microsoft Windows Vista, 7 o Server 2008 con privilegios administrativos.
2. Haga clic en **Start** > **Run**.
3. Escriba **gpedit.msc**.
4. Vaya a **Computer Configuration** > **Administrative Templates** > **System** > **Device Installation**.
5. Haga clic con el botón secundario en **Allow remote access to the PnP interface** y seleccione **Properties**.
6. En la ficha **Settings**, seleccione la opción **Enable**.
7. Haga clic en **Ok** para guardar los cambios.
8. Reinicie el equipo.

Para ejecutar un examen de dispositivos:

1. Haga clic en la ficha **Scanning.**
2. En **Common tasks**, haga clic en **Options**.
3. En el cuadro de diálogo **Options**, seleccione la ficha **Logon Credentials.**



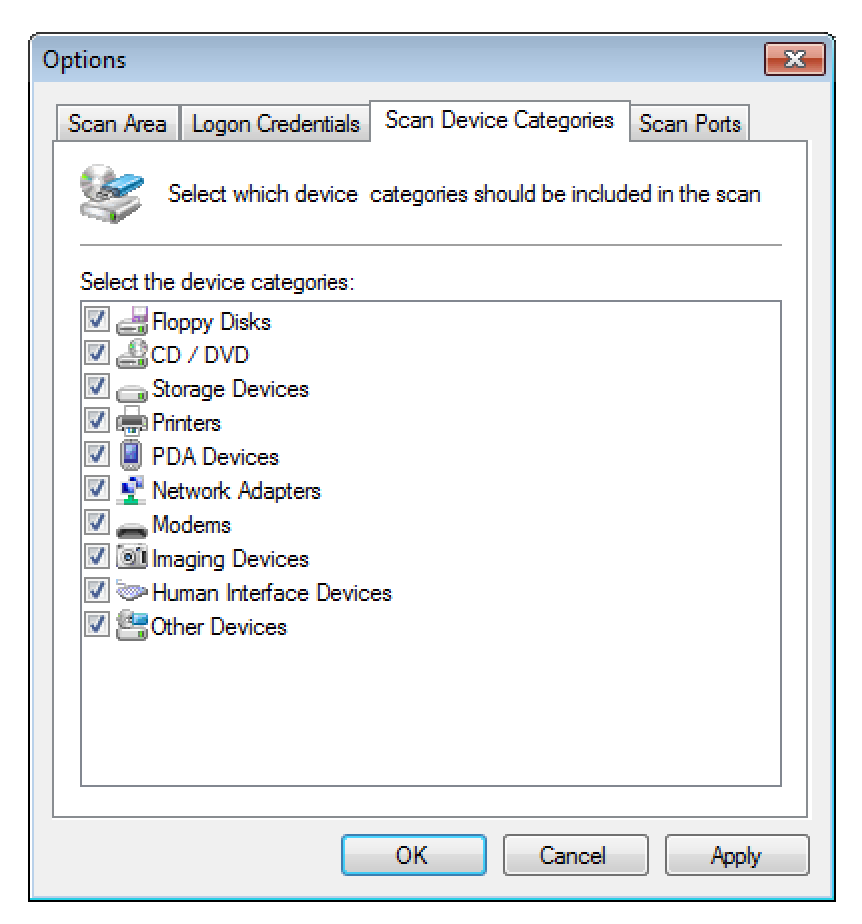
Captura de pantalla 74: Ejecución de un examen de dispositivos: Ficha Logon credentials

4. En la ficha **Logon Credentials** del cuadro de diálogo **Options**, seleccione o anule la selección de **Logon using credentials below** para habilitar o deshabilitar el uso de credenciales alternativas.



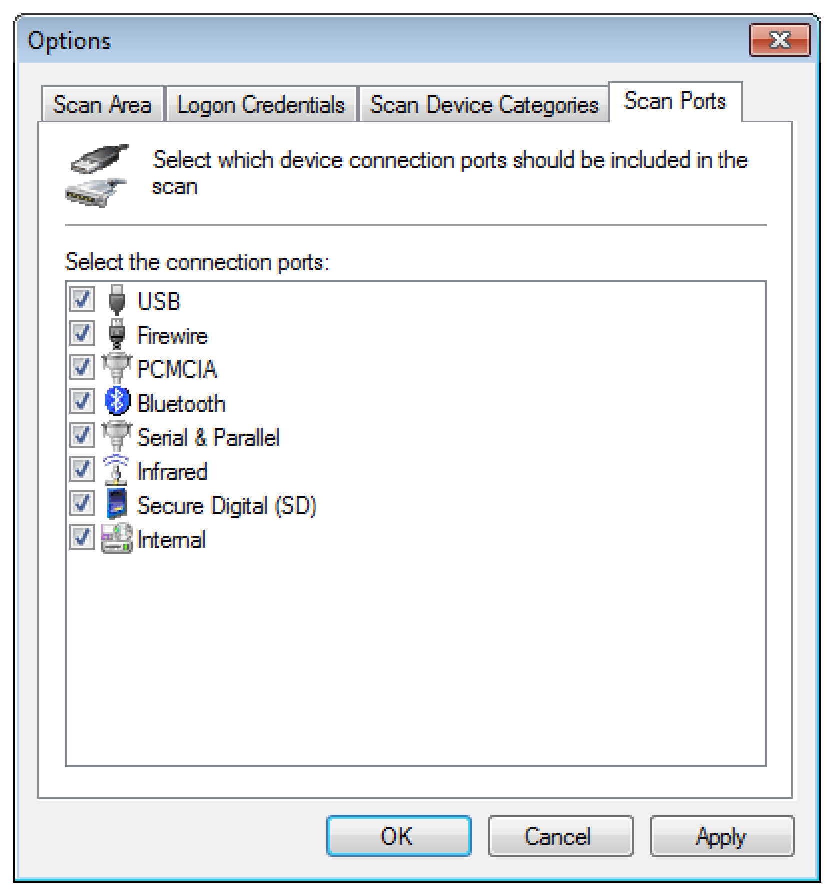
Nota

Si no especifica credenciales de inicio de sesión, GFI EndPointSecurity intenta iniciar sesión en el equipo de destino con el usuario de la sesión actual.



Captura de pantalla 75: Ejecución de un examen de dispositivos: Ficha Scan device categories

5. Haga clic en la ficha **Scan Device Categories** y seleccione las categorías de dispositivos que desee incluir en el examen.



Captura de pantalla 76: Ejecución de un examen de dispositivos: Ficha Scan ports

6. Haga clic en la ficha **Scan Ports** y seleccione los puertos de conexión que desee incluir en el examen.
7. Haga clic en **Apply** y en **OK**.
8. Para especificar equipos de destino para el examen:

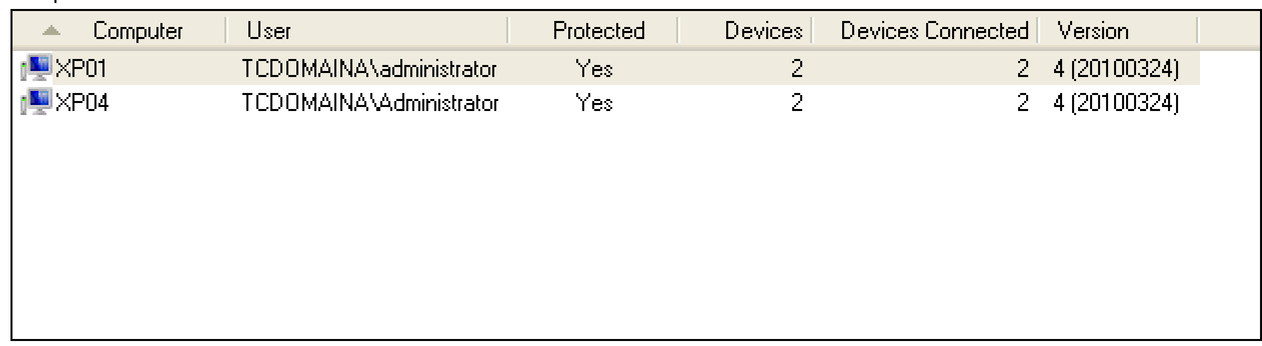
- En el panel derecho, escriba el nombre de equipo o la dirección IP de los equipos de destino en el cuadro de texto **Scan target**. Haga clic en **New Scan** para comenzar a examinar el equipo especificado.

7.2 Análisis de los resultados del examen de dispositivos

Los resultados del examen dispositivos se muestran en dos secciones:

- Computers
- Devices list

7.2.1 Computers


Computers:

Computer	User	Protected	Devices	Devices Connected	Version
XP01	TCDOMAINA\administrator	Yes	2	2	4 (20100324)
XP04	TCDOMAINA\Administrator	Yes	2	2	4 (20100324)

Captura de pantalla 77: Área Computers

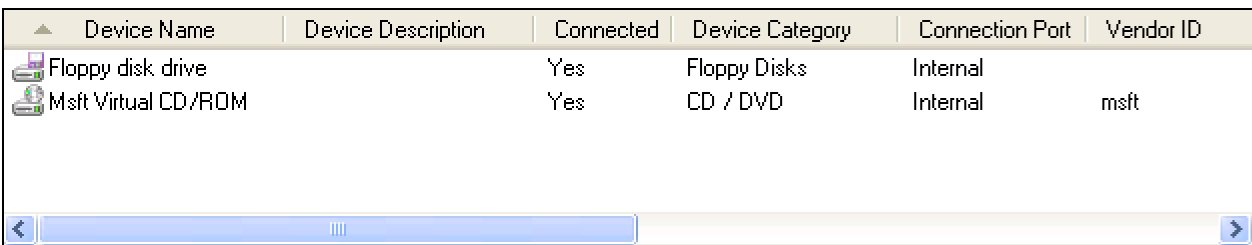
En esta sección, se muestran los resultados del resumen del examen de dispositivos para cada equipo de destino examinado, en los que se incluyen:

- Nombre de equipo/dirección IP
- Usuario de la sesión actual
- Estado de protección, es decir, si el equipo está incluido en una directiva de protección de GFI EndPointSecurity
- Número total de dispositivos actual e históricamente conectados
- Número de dispositivos actualmente conectados.

Si un equipo de destino examinado no está incluido en ninguna directiva de protección de GFI EndPointSecurity, puede elegir implementar una directiva de protección en el equipo. Para ello:

1. En la columna **Computer**, haga clic con el botón secundario en el nombre de equipo/dirección IP relevante y seleccione **Deploy agent(s)…**
2. Seleccione la directiva de protección que desee implementar. Haga clic en **Next** para continuar y en **Finish** para comenzar la implementación.

7.2.2 Devices list


Devices list:

Device Name	Device Description	Connected	Device Category	Connection Port	Vendor ID
Floppy disk drive		Yes	Floppy Disks	Internal	
Msft Virtual CD/ROM		Yes	CD / DVD	Internal	msft

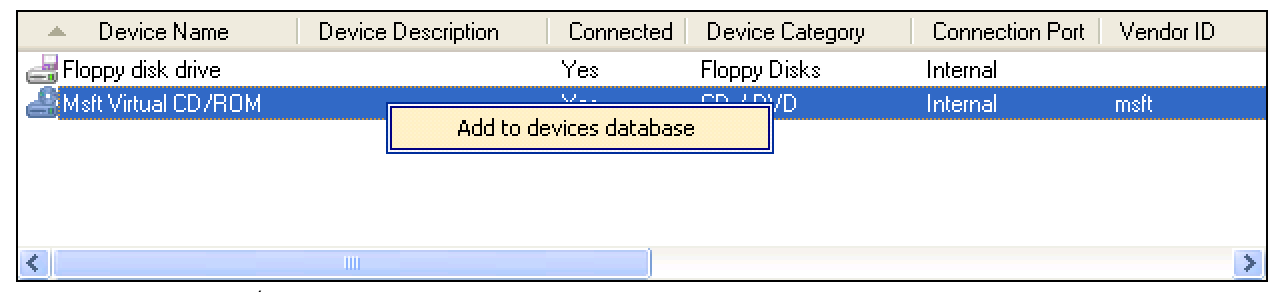
Captura de pantalla 78: Área Devices list

En esta sección, se muestra una lista detallada de los dispositivos detectados para cada equipo examinado, que incluye:

- Nombre de dispositivo, descripción y categoría
- Puerto de conectividad
- Estado de conexión, es decir, si el dispositivo está conectado actualmente o no.

7.3 Incorporación de los dispositivos detectados a la base de datos

Puede seleccionar uno o más de los dispositivos detectados de la lista **Devices** y agregarlos a la base de datos de dispositivos. A continuación, estos dispositivos se recuperan desde esta base de datos cuando GFI EndPointSecurity muestra los dispositivos actualmente conectados a los equipos de destino para la lista negra y la lista blanca. Para obtener información, consulte Configuración de una lista negra de dispositivos o Configuración de una lista blanca de dispositivos.



Captura de pantalla 79: Área Devices list: Agregar un dispositivo a la base de datos de dispositivos

Para agregar dispositivos a la base de datos de dispositivos:

1. Seleccione uno o más dispositivos para agregar a la base de datos de dispositivos desde la sección **Devices**.
2. Haga clic con el botón secundario en los dispositivos seleccionados y seleccione **Add to devices database**.
3. Haga clic en **OK**.

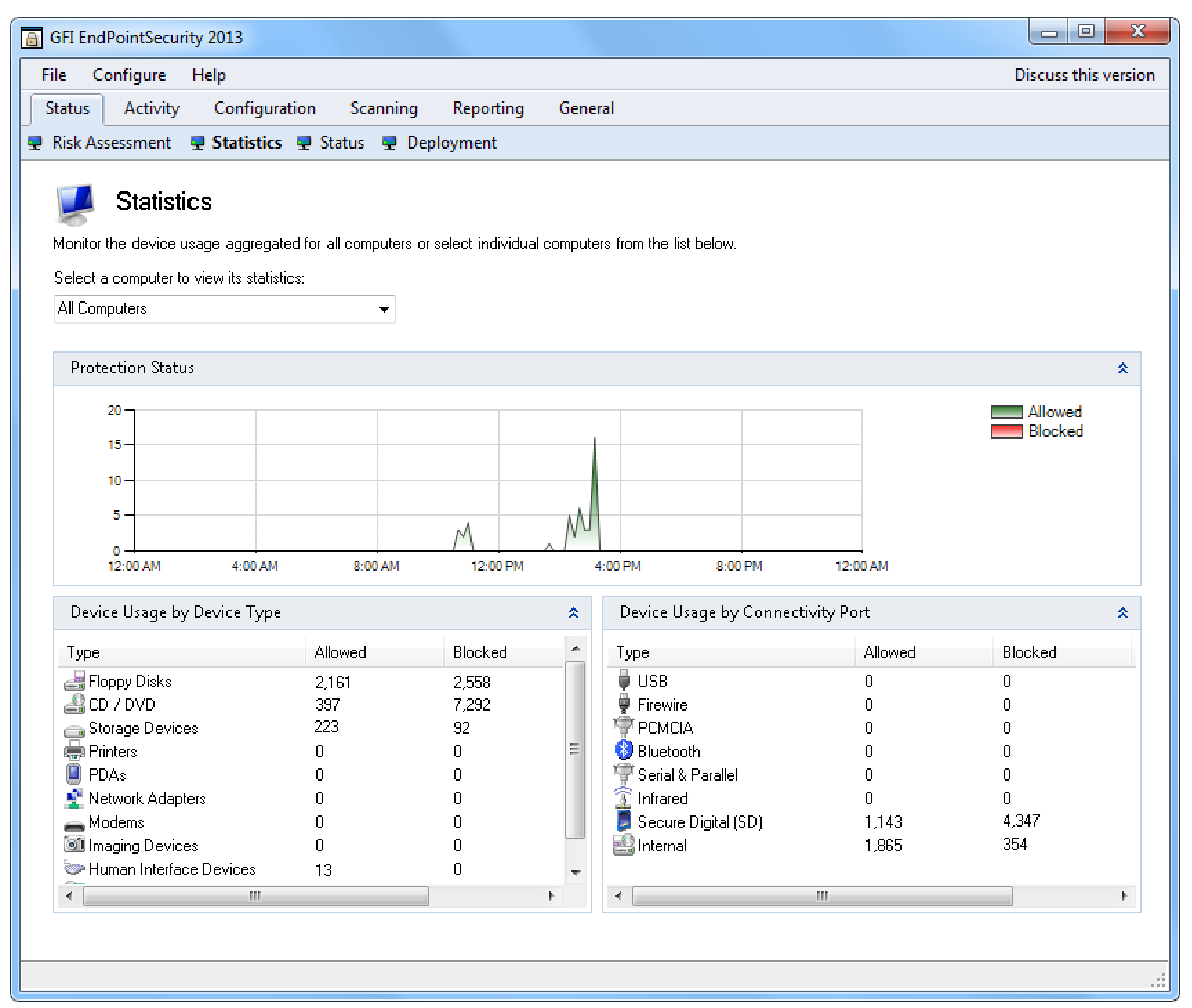
8 Supervisión de la actividad de uso de dispositivos

En este capítulo, se brinda información acerca de la supervisión de la actividad de sus dispositivos de red. GFI EndPointSecurity le permite realizar un seguimiento de las auditorías de todos los eventos generados por los agentes de GFI EndPointSecurity implementados en los equipos de red. Para realizar un seguimiento de auditoría, debe habilitar el registro. Para obtener más información, consulte Configuración del registro de eventos (página 96).

Temas de este capítulo

8.1 Estadísticas

Use la subficha Statistics para ver las tendencias de actividad diaria de los dispositivos y estadísticas de un equipo específico o de todos los equipos de red.



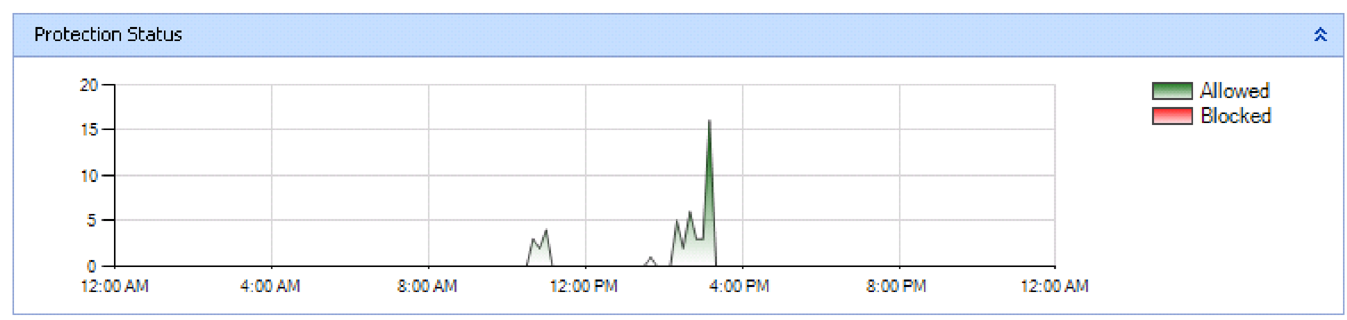
Captura de pantalla 80: Subficha Statistics

Para acceder a la subficha Statistics, en la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Status > Statistics**.

La sección **Statistics** contiene información acerca de:

- Estado de protección
- Uso de dispositivos por tipo de dispositivo
- Uso de dispositivos por puerto de conectividad

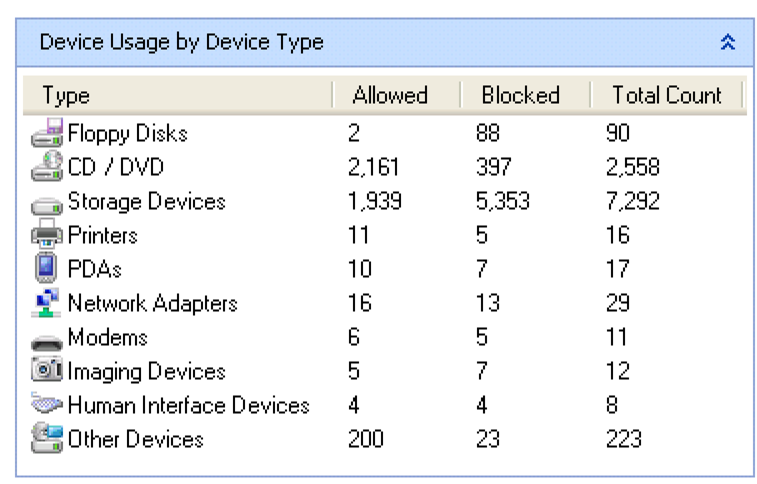
8.1.1 Estado de protección



Captura de pantalla 81: Área Protection Status

En esta sección se representa gráficamente el uso diario de dispositivos en los equipos de red, diferenciando entre los dispositivos bloqueados y aquellos habilitados por los agentes. La información proporcionada se puede filtrar para un equipo específico o para todos los equipos de red:

8.1.2 Uso de dispositivos por tipo de dispositivo



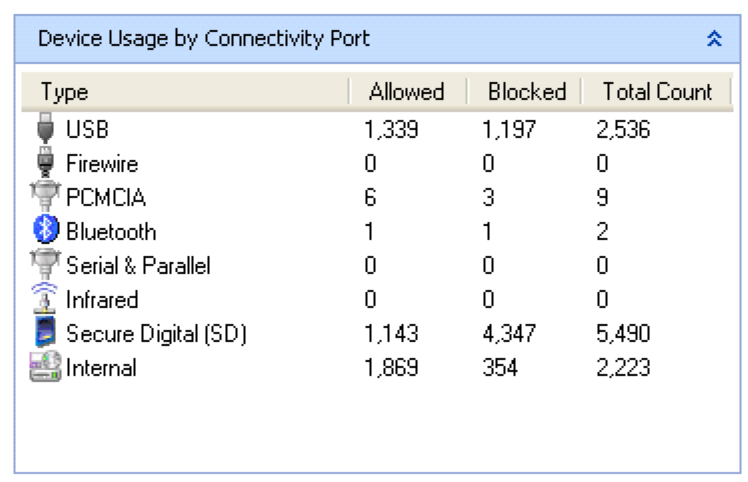
Device Usage by Device Type

Type	Allowed	Blocked	Total Count
Floppy Disks	2	88	90
CD / DVD	2,161	397	2,558
Storage Devices	1,939	5,353	7,292
Printers	11	5	16
PDAs	10	7	17
Network Adapters	16	13	29
Modems	6	5	11
Imaging Devices	5	7	12
Human Interface Devices	4	4	8
Other Devices	200	23	223

Captura de pantalla 82: Área Device Usage by Device Type

En esta sección, se enumeran los intentos de conexión a dispositivos por tipo de dispositivo, y si fueron permitidos o bloqueados. La información proporcionada se puede filtrar para un equipo específico o para todos los equipos de red:

8.1.3 Uso de dispositivos por puerto de conectividad



Type	Allowed	Blocked	Total Count
USB	1,339	1,197	2,536
Firewire	0	0	0
PCMCIA	6	3	9
Bluetooth	1	1	2
Serial & Parallel	0	0	0
Infrared	0	0	0
Secure Digital (SD)	1,143	4,347	5,490
Internal	1,869	354	2,223

Captura de pantalla 83: Área Device Usage by Connectivity Port

En esta sección, se enumeran los intentos de conexión a dispositivos por puerto de conectividad, y si fueron permitidos o bloqueados. La información proporcionada se puede filtrar para un equipo específico o para todos los equipos de red:

8.2 Actividad

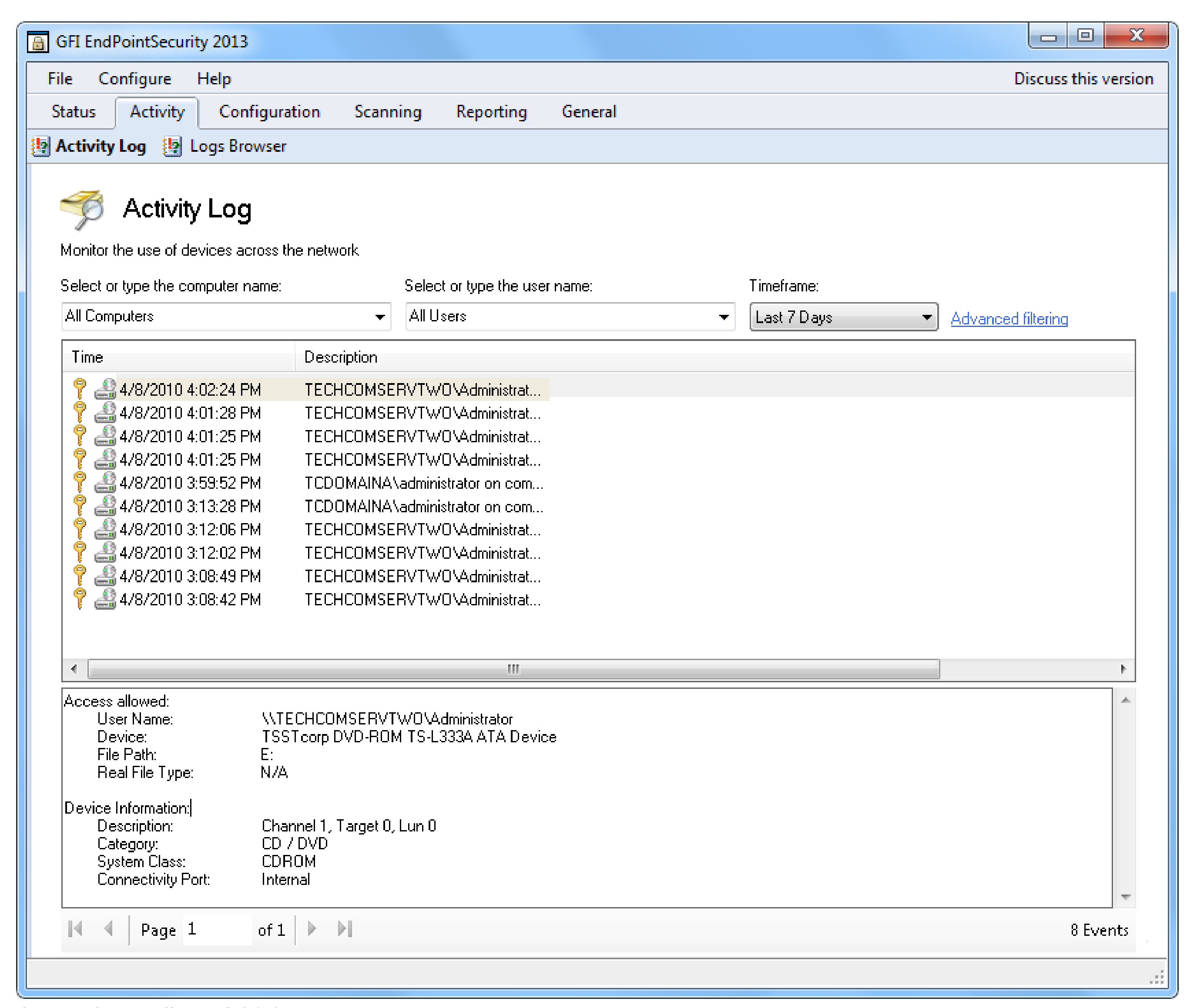
Use la ficha Activity para supervisar el uso de dispositivos en la red y los eventos registrados de un equipo específico o de todos los equipos de red.

La sección Activity contiene información acerca de:

- Registro de actividades
- Filtrado avanzado
- Explorador de registros
- Creación de consultas de eventos

8.2.1 Registro de actividades

Esta subficha le permite supervisar los dispositivos en uso en la red. Seleccione el equipo o el usuario de las listas desplegables relevantes para filtrar la lista Activity Log por equipo o por usuario. Además, esta ficha le permite filtrar aún más la lista con los filtros de tiempo proporcionados.



Captura de pantalla 84: Subficha Activity Log

Para acceder a la subficha Activity Log, en la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Activity** > **Activity Log**.

Para ver más detalles acerca de un evento en particular, haga clic en el evento. En el panel de descripción de eventos de la parte inferior de la subficha se muestra información adicional.

Para personalizar la subficha Activity Log para que se ajuste a las necesidades de su compañía, haga clic con el botón secundario en el encabezado y seleccione las columnas que deben agregarse o quitarse de la vista.

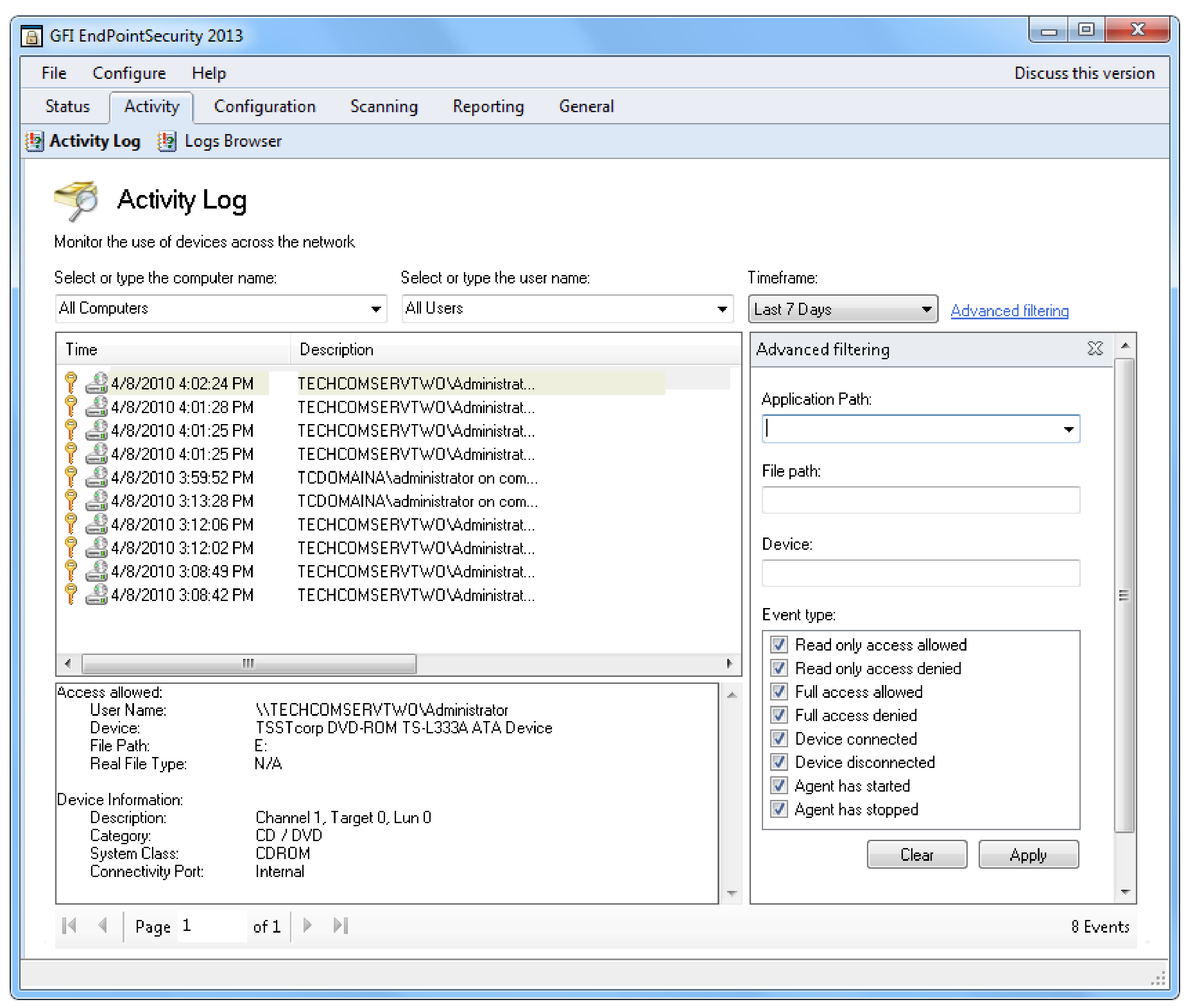
Para cambiar la posición de una columna, seleccione el encabezado de la columna, arrástrelo a la posición deseada y suéltelo.

8.2.2 Advanced Filtering

Esta función le permite filtrar aún más los registros del historial de uso de dispositivos mediante uno o más criterios del siguiente conjunto:

- Ruta de aplicación
- Ruta de archivo

- Dispositivo
- Tipo de evento.



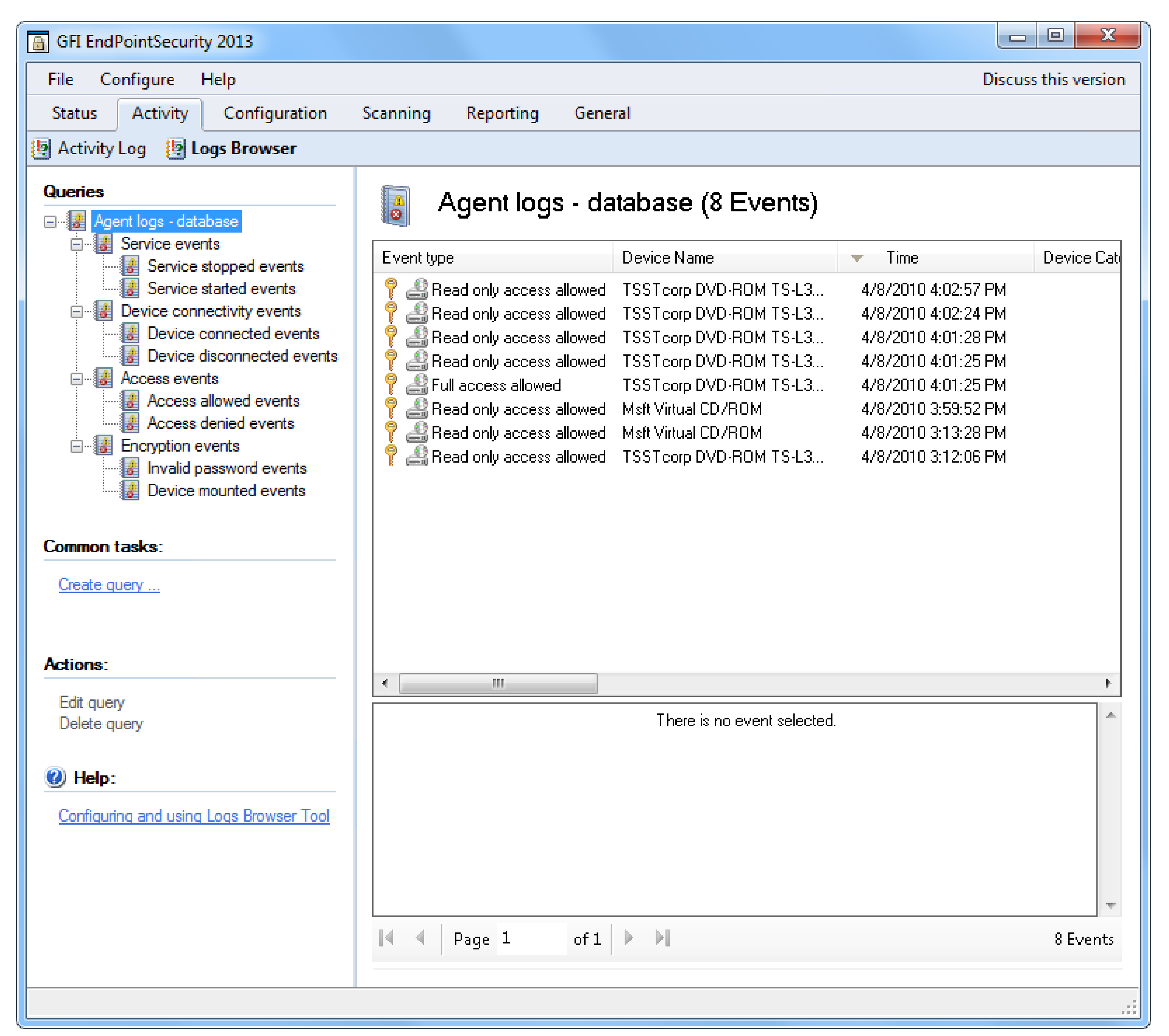
Captura de pantalla 85: Subficha Activity Log: Filtrado avanzado

Para acceder a las opciones de filtrado avanzado del registro de actividad, haga clic en **Advanced filtering** en la subficha **Activity Log**.

8.2.3 Logs Browser

La subficha Logs Browser le permite acceder y examinar eventos actualmente almacenados en el back-end de base de datos.

GFI EndPointSecurity también incluye un generador de consultas para simplificar la búsqueda de eventos específicos. Con el generador de consultas de eventos, puede crear filtros personalizados que filtren los datos sobre eventos y muestren únicamente la información que necesita examinar, sin eliminar registros de su back-end de base de datos.



Captura de pantalla 86: Subficha Logs Browser

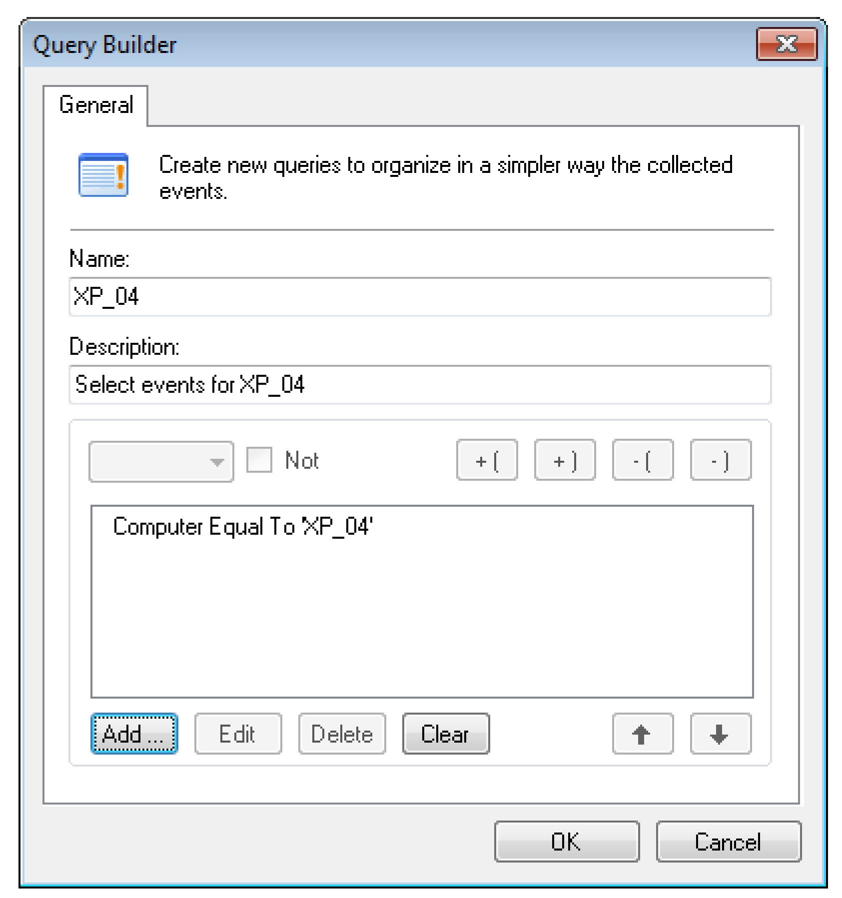
Para acceder a la subficha Logs Browser, en la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Activity** > **Logs Browser**.

Para ver más detalles acerca de un evento en particular, haga clic en el evento. En el panel de descripción de eventos de la parte inferior de la subficha se muestra información adicional.

8.2.4 Creación de consultas de eventos

Para crear consultas de eventos personalizadas:

1. En la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Activity**.
2. Haga clic en la subficha **Logs Browser**.
3. En el panel izquierdo, haga clic con el botón secundario en el nodo **Agent logs - database** y seleccione **Create query...**.



Captura de pantalla 87: Opciones del generador de consultas

4. En el cuadro de diálogo **Query Builder**, especifique un nombre y una descripción para la nueva consulta.
5. Haga clic en **Add…**, configure las condiciones de consulta necesarias y haga clic en **OK**. Repita estos pasos hasta que se hayan especificado todas las condiciones de consulta necesarias.
6. Haga clic en **OK** para finalizar la configuración. La consulta personalizada se agrega como un subnodo dentro del nodo **Agent logs - database**.



Nota

También puede filtrar los resultados de las consultas de eventos existentes creando consultas secundarias más específicas. Para hacer esto, haga clic con el botón secundario en una consulta y seleccione **Create query…**.

9 Supervisión de estado

En este capítulo, se proporciona información relacionada con la supervisión del estado de GFI EndPointSecurity y de los agentes de GFI EndPointSecurity. Las vistas de estado le proporcionan información estadística y gráficos relacionados con el uso de dispositivos.

Temas de este capítulo

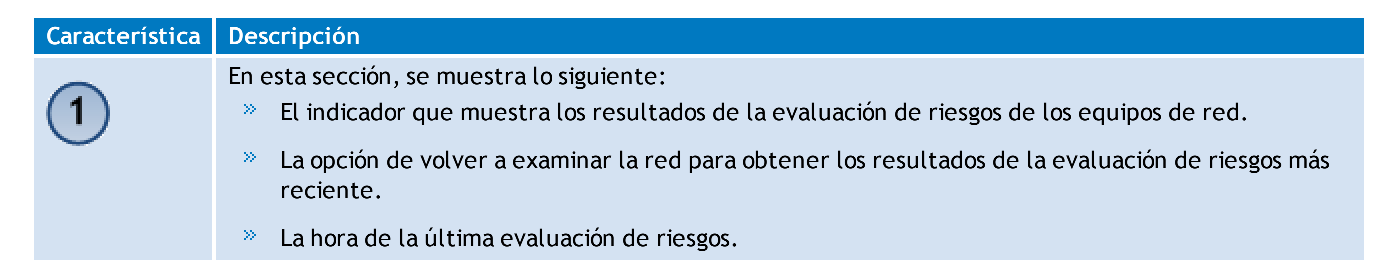
9.1 Vista de evaluación de riesgos

Use la subficha Risk Assessment para ver el estado de lo siguiente:

- El nivel de evaluación de riesgos en los equipos de red con agentes de GFI EndPointSecurity instalados en ellos.
- Los agentes de GFI EndPointSecurity implementados en los equipos de red.
- El uso de dispositivos, como el número y el porcentaje de dispositivos bloqueados y el número de dispositivos habilitados.
- El nivel de amenaza de los dispositivos en la red.

Captura de pantalla 88: Subficha Risk Assessment

Para acceder a la subficha Risk Assessment, en la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Status > Risk Assessment**.



Característica	Descripción
1	En esta sección, se muestra lo siguiente: » El indicador que muestra los resultados de la evaluación de riesgos de los equipos de red. » La opción de volver a examinar la red para obtener los resultados de la evaluación de riesgos más reciente. » La hora de la última evaluación de riesgos.

Característica	Descripción
2	En esta sección, se muestran los valores acumulativos del número de: » Extremos examinados » Exámenes correctos » Extremos protegidos » Extremos no protegidos » Dispositivos detectados En esta sección, también se representa lo siguiente: » La red donde están instalados los agentes » La fecha y hora de la última evaluación de riesgos.
3	En esta sección se representa gráficamente el número de agentes que actualmente: » Están esperando la instalación en los equipos de red » Están protegidos con GFI EndPointSecurity » No están protegidos con GFI EndPointSecurity
4	En esta sección se representan gráficamente todos los agentes implementados en los equipos de red, diferenciando entre aquellos que actualmente están en línea y los que están desconectados. Para obtener más información, consulte Vista de estado (página 119).
5	En esta sección se representan gráficamente los niveles de porcentaje de amenazas de dispositivos según lo registrado por los agentes de los equipos de red que tienen GFI EndPointSecurity instalado.
6	En esta sección se representan gráficamente los porcentajes de accesos de usuarios por categoría de dispositivo de la cantidad total acumulativa de accesos de usuarios a dispositivos, según los registros de los agentes. Los accesos de usuarios a dispositivos hacen referencia a accesos bloqueados y habilitados.
7	En esta sección, se muestra lo siguiente: » La cuenta de usuario en la que se está ejecutando el servicio de GFI EndPointSecurity. » El nivel de factor de riesgo. » El estado de cifrado actual en el extremo. » El estado de la función de comprobación de tipo de archivo. » El estado de la función de comprobación de contenido.

9.2 Vista de estadísticas

Use la subficha Statistics para ver las tendencias de actividad diaria de los dispositivos y estadísticas de un equipo específico o de todos los equipos de red.

GFI EndPointSecurity 2013

File Configure Help Discuss this version

Status Activity Configuration Scanning Reporting General

Risk Assessment **Statistics** Status Deployment

Statistics

Monitor the device usage aggregated for all computers or select individual computers from the list below.

Select a computer to view its statistics:

All Computers

Protection Status

20
15
10
5
0
12:00 AM 4:00 AM 8:00 AM 12:00 PM 4:00 PM 8:00 PM 12:00 AM

Allowed
Blocked

Device Usage by Device Type

Type	Allowed	Blocked
Floppy Disks	2,161	2,558
CD / DVD	397	7,292
Storage Devices	223	92
Printers	0	0
PDAs	0	0
Network Adapters	0	0
Modems	0	0
Imaging Devices	0	0
Human Interface Devices	13	0

Device Usage by Connectivity Port

Type	Allowed	Blocked
USB	0	0
Firewire	0	0
PCMCIA	0	0
Bluetooth	0	0
Serial & Parallel	0	0
Infrared	0	0
Secure Digital (SD)	1,143	4,347
Internal	1,865	354

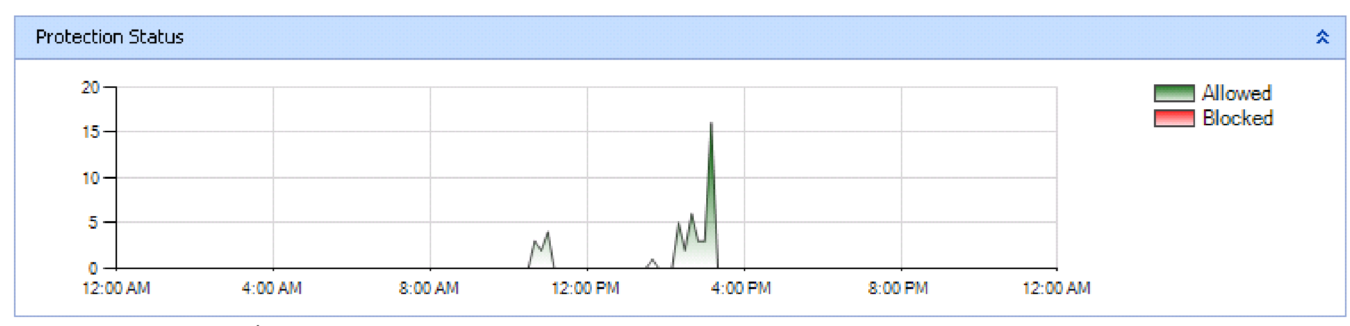
Captura de pantalla 89: Subficha Statistics

Para acceder a la subficha Statistics, en la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Status > Statistics.**

La sección **Statistics** contiene información acerca de:

- Estado de protección
- Uso de dispositivos por tipo de dispositivo
- Uso de dispositivos por puerto de conectividad

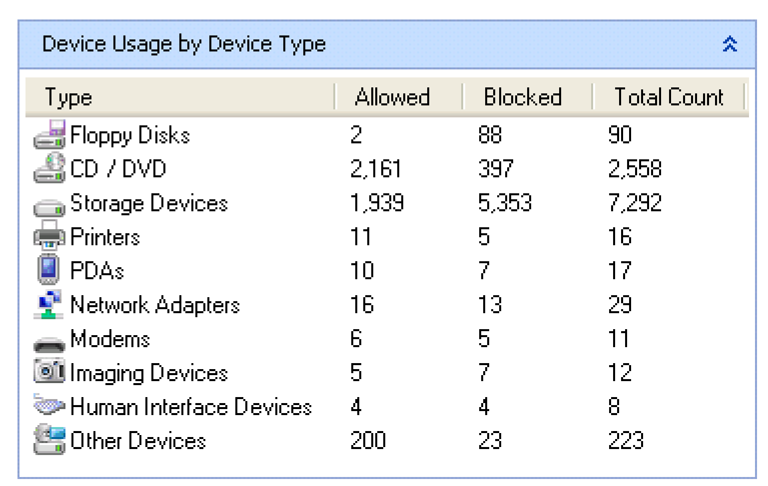
9.2.1 Estado de protección



Captura de pantalla 90: Área Protection Status

En esta sección se representa gráficamente el uso diario de dispositivos en los equipos de red, diferenciando entre los dispositivos bloqueados y aquellos habilitados por los agentes. La información proporcionada se puede filtrar para un equipo específico o para todos los equipos de red:

9.2.2 Uso de dispositivos por tipo de dispositivo

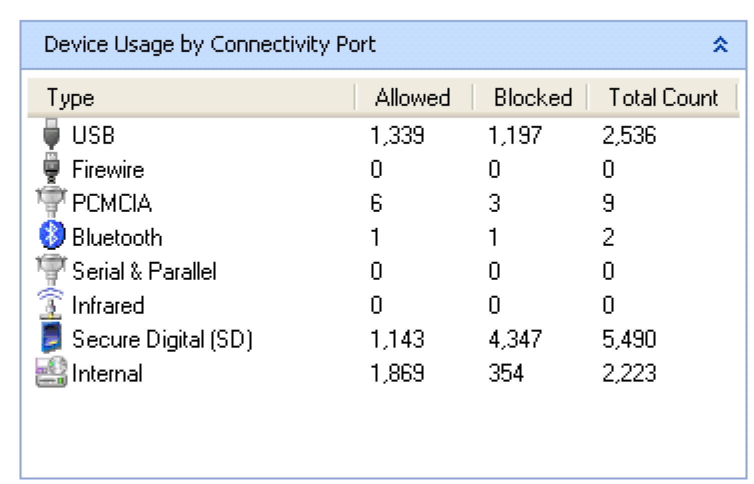

Device Usage by Device Type

Type	Allowed	Blocked	Total Count
Floppy Disks	2	88	90
CD / DVD	2,161	397	2,558
Storage Devices	1,939	5,353	7,292
Printers	11	5	16
PDAs	10	7	17
Network Adapters	16	13	29
Modems	6	5	11
Imaging Devices	5	7	12
Human Interface Devices	4	4	8
Other Devices	200	23	223

Captura de pantalla 91: Área Device Usage by Device Type

En esta sección, se enumeran los intentos de conexión a dispositivos por tipo de dispositivo, y si fueron permitidos o bloqueados. La información proporcionada se puede filtrar para un equipo específico o para todos los equipos de red:

9.2.3 Uso de dispositivos por puerto de conectividad


Device Usage by Connectivity Port

Type	Allowed	Blocked	Total Count
USB	1,339	1,197	2,536
Firewire	0	0	0
PCMCIA	6	3	9
Bluetooth	1	1	2
Serial & Parallel	0	0	0
Infrared	0	0	0
Secure Digital (SD)	1,143	4,347	5,490
Internal	1,869	354	2,223

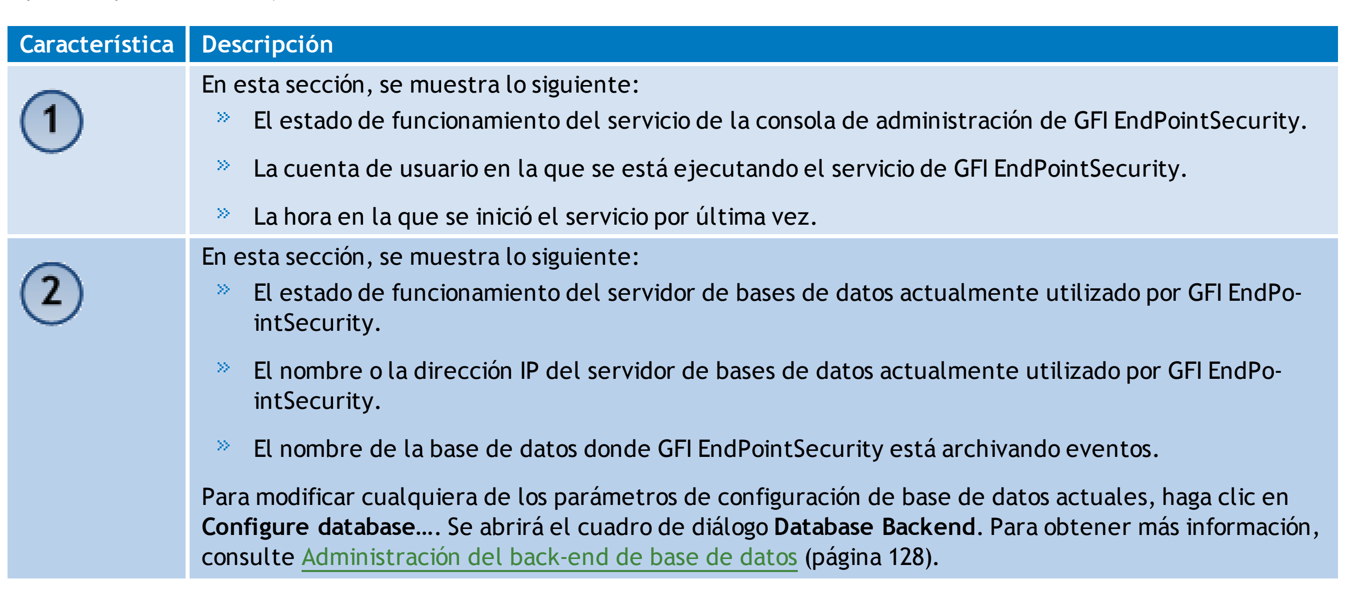
Captura de pantalla 92: Área Device Usage by Connectivity Port

En esta sección, se enumeran los intentos de conexión a dispositivos por puerto de conectividad, y si fueron permitidos o bloqueados. La información proporcionada se puede filtrar para un equipo específico o para todos los equipos de red:

9.3 Vista de estado

Use la subficha Status para determinar el estado de todas las operaciones de implementación realizadas en sus destinos de red. La información que se muestra incluye lo siguiente sobre cada equipo de destino:

Captura de pantalla 93: Subficha Status

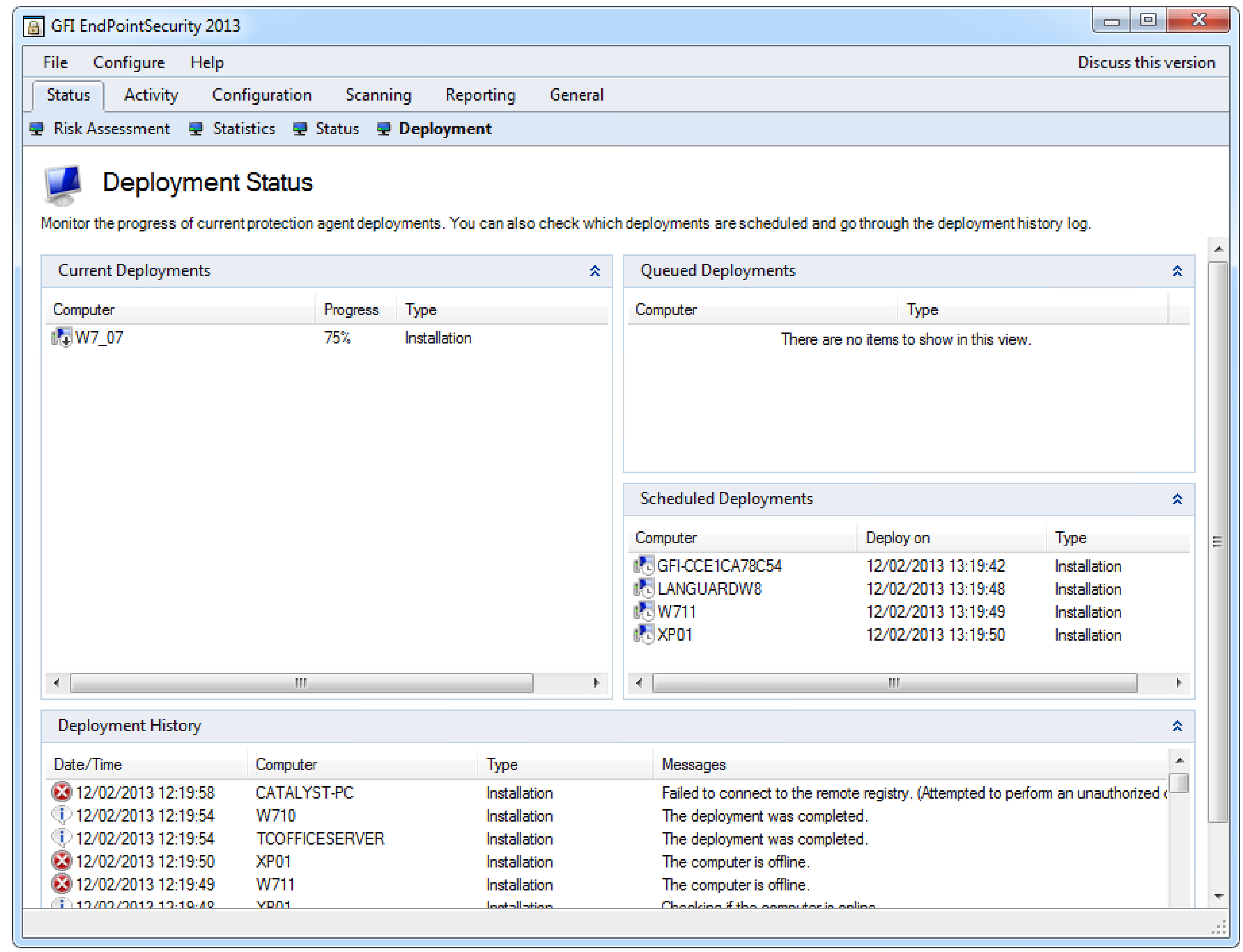


Característica	Descripción
1	En esta sección, se muestra lo siguiente: » El estado de funcionamiento del servicio de la consola de administración de GFI EndPointSecurity. » La cuenta de usuario en la que se está ejecutando el servicio de GFI EndPointSecurity. » La hora en la que se inició el servicio por última vez.
2	En esta sección, se muestra lo siguiente: » El estado de funcionamiento del servidor de bases de datos actualmente utilizado por GFI EndPointSecurity. » El nombre o la dirección IP del servidor de bases de datos actualmente utilizado por GFI EndPointSecurity. » El nombre de la base de datos donde GFI EndPointSecurity está archivando eventos. Para modificar cualquiera de los parámetros de configuración de base de datos actuales, haga clic en **Configure database...**. Se abrirá el cuadro de diálogo **Database Backend**. Para obtener más información, consulte Administración del back-end de base de datos (página 128).

Característica	Descripción
3	En esta sección, se muestra lo siguiente: » El estado de funcionamiento del servidor de alertas actualmente utilizado por GFI EndPointSecurity. » El nombre o la dirección IP del servidor de alertas actualmente utilizado por GFI EndPointSecurity. Para modificar cualquiera de los parámetros de configuración relacionados con las alertas actuales, haga clic en **Configure alerting…**. Se iniciará el cuadro de diálogo **Alerting Options**. Para obtener más información, consulte Configuración de alertas (página 98).
4	En esta sección se representan gráficamente todos los agentes implementados en los equipos de red, diferenciando entre aquellos que actualmente están en línea y los que están desconectados.
5	En esta selección, se muestra lo siguiente: » El nombre del equipo de destino y la directiva de protección correspondiente. » El estado del agente de GFI EndPointSecurity, si actualmente está implementado y actualizado o si está esperando implementación. » El estado del equipo de destino, si actualmente está en línea o desconectado. Para implementar agentes pendientes: 1. Seleccione uno o más equipos de **Agents' Status**. 2. Haga clic con el botón secundario en los equipos seleccionados y elija **Deploy selected agent(s)** o **Schedule deployment for selected agent(s)…**. 3. Haga clic en **OK**. **Nota** Si un equipo de destino está desconectado, la implementación difiere por una hora. GFI EndPointSecurity intenta implementar esa directiva cada hora, hasta que el equipo de destino se vuelve a conectar. **Nota** Cada agente envía su estado en línea a GFI EndPointSecurity a intervalos regulares. Si la aplicación principal no recibe estos datos, el agente se considera desconectado.

9.4 Vista del estado de implementación

9.4.1 Acerca de la vista del estado de implementación



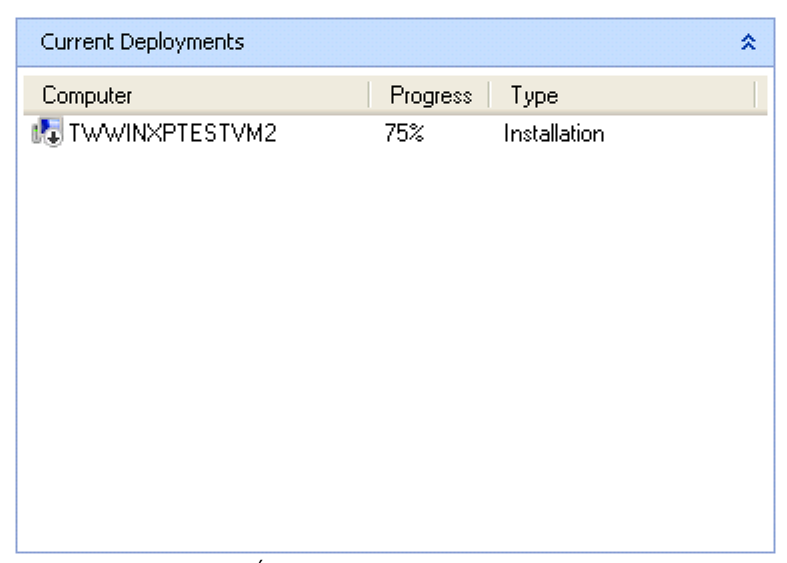
Captura de pantalla 94: Subficha Deployment

Use la subficha Deployment para ver lo siguiente:

- Actividad de implementación actual
- Implementaciones en cola
- Implementaciones programadas
- Historial de implementaciones.

Para acceder a la subficha Deployment, en la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Status** > **Deployment**.

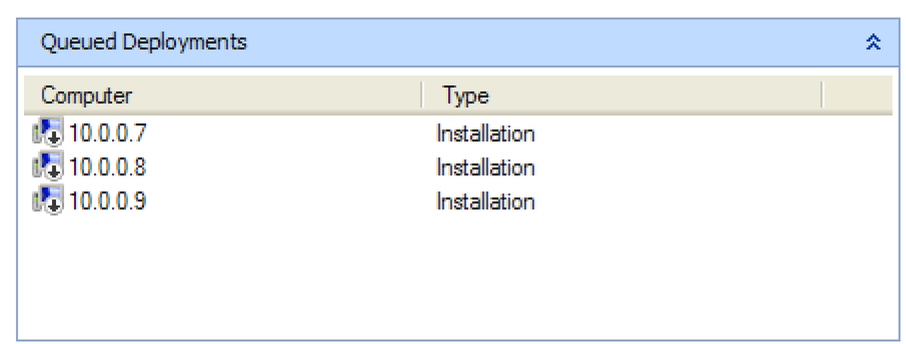
9.4.2 Implementaciones actuales



Captura de pantalla 95: Área Current Deployments

En esta sección, se muestra una lista de las implementaciones que se están realizando actualmente. La información proporcionada incluye el nombre del equipo, el progreso de la implementación y el tipo de implementación. La implementación es una instalación, una desinstalación o una actualización.

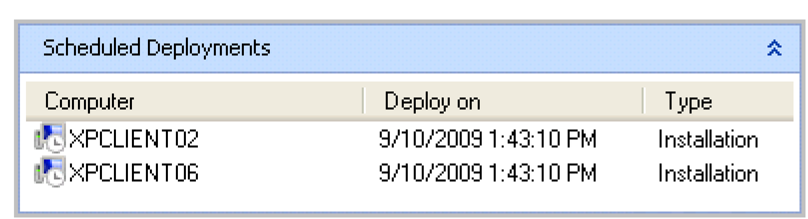
9.4.3 Implementaciones en cola



Captura de pantalla 96: Área Queued Deployments

En esta sección, se muestra una lista de implementaciones pendientes. La información proporcionada incluye el nombre del equipo y el tipo de implementación.

9.4.4 Implementaciones programadas



Captura de pantalla 97: Área Scheduled Deployments

En esta sección, se muestra una lista de implementaciones programadas. La información proporcionada incluye el nombre del equipo, el horario de programación y el tipo de implementación.

9.4.5 Historial de implementación

Deployment History

Date/Time	Computer	Type	Messages
4/8/2010 4:52:38 PM	XP04	Installation	The deployment was completed.
4/8/2010 4:52:33 PM	XP04	Installation	Installing the protection agent...
4/8/2010 4:52:33 PM	XP04	Installation	Installing the deployment service...
4/8/2010 4:52:32 PM	XP04	Installation	Copying the setup files...
4/8/2010 4:52:32 PM	XP04	Installation	Preparing files...
4/8/2010 4:52:32 PM	XP04	Installation	Collecting information...
4/8/2010 4:52:32 PM	XP04	Installation	Checking if the computer is online...
4/8/2010 4:52:23 PM	XP04	Un-installation	The un-installation was completed.
4/8/2010 4:52:14 PM	XP04	Un-installation	Un-installing the protection agent

Captura de pantalla 98: Área Deployment History

En esta sección, se muestra un seguimiento de auditoría para todas las etapas de todas las implementaciones de directivas de protección o agentes llevadas a cabo por GFI EndPointSecurity. La información proporcionada incluye la marca de hora de cada entrada de registro, el nombre del equipo, el tipo de implementación y los mensajes de error y de información generados durante el proceso de implementación. Para obtener más información, consulte Solución de problemas y asistencia técnica (página 150).

Para quitar las entradas de registro mostradas, haga clic con el botón secundario en el área **Deployment History** y seleccione **Clear all messages**.

10 Generación de informes

GFI EndPointSecurity GFI ReportPack es un complemento de informe integral de GFI EndPointSecurity. Este paquete de informes puede programarse para que genere automáticamente informes gráficos de administración y de TI en función de los datos recopilados por GFI EndPointSecurity, lo cual le ofrece la capacidad de informar sobre dispositivos conectados a la red, tendencias de uso de dispositivos por equipo o por usuario, archivos copiados desde y hacia dispositivos (incluidos los nombres reales de los archivos copiados) y mucho más.

Temas de este capítulo

10.1 GFI EndPointSecurity GFI ReportPack

Para generar informes, debe descargar e instalar el complemento de GFI EndPointSecurity GFI ReportPack. Para descargar el complemento, visite: http://www.gfi.com/endpointsecurity/esecreportpack.htm

Para obtener más información sobre GFI EndPointSecurity GFI ReportPack:

1. Haga clic en la ficha **Reporting**.
2. En el panel izquierdo, seleccione **GFI EndPointSecurity GFI ReportPack** o **GFI ReportCenter**.



Nota

Se requiere una conexión a Internet.

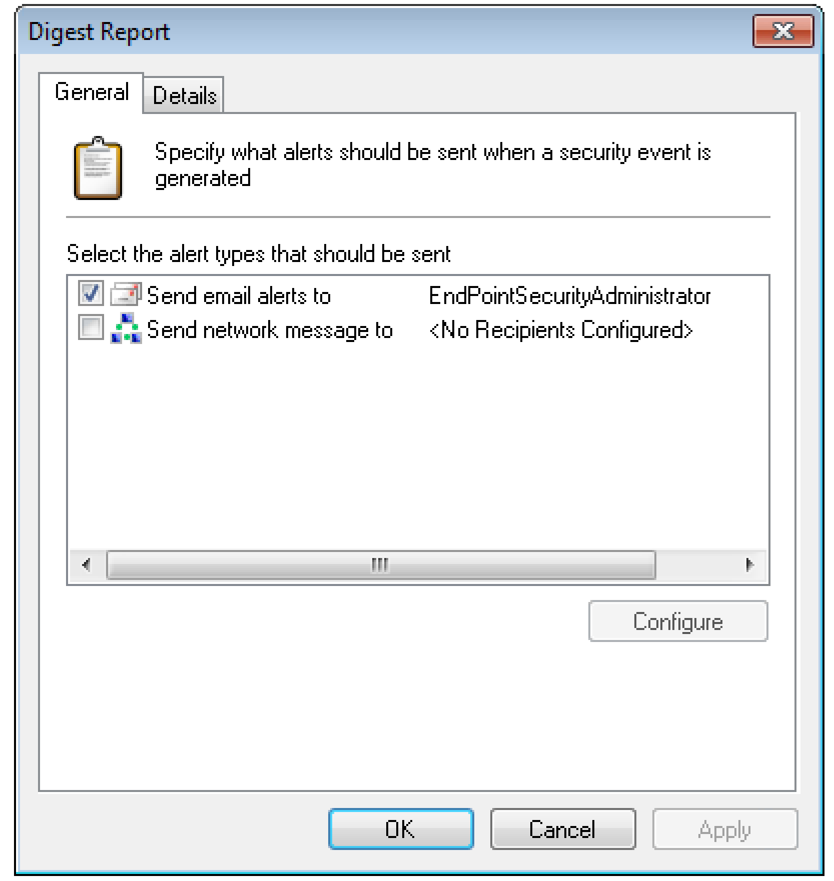
10.2 Generación de informes de resumen

GFI EndPointSecurity le permite generar informes de resumen para los destinatarios configurados. Los informes de resumen contienen una síntesis de las estadísticas de actividad periódica según lo detectado por GFI EndPointSecurity.

Los destinatarios de alertas no son usuarios o grupos de usuarios de Active Directory (AD), sino que son cuentas de perfil creadas por GFI EndPointSecurity para contener los detalles de contacto de los usuarios a los que se destinan las alertas. Es mejor crear los destinatarios de las alertas antes de configurar las alertas. Para obtener más información, consulte Configuración de destinatarios de alertas (página 138).

Para configurar informes de resumen:

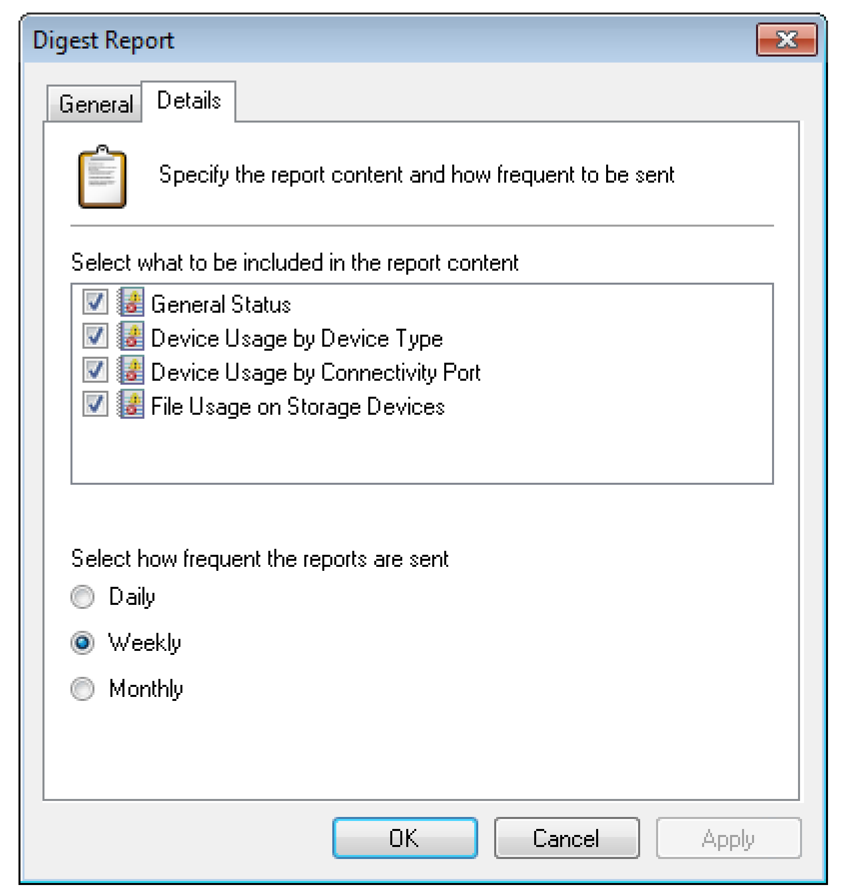
1. Haga clic en la ficha **Configuration**, subficha > **Options**.
2. En **Configure**, haga clic en **Alerting Options** y, en el panel derecho, haga clic en **Configure the digest report**.



Captura de pantalla 99: Opciones de Digest Report: Ficha General

3. En la ficha **General** del cuadro de diálogo **Digest Report**, seleccione o anule la selección del método de alerta que prefiera.

4. Para cada tipo de alerta seleccionado, haga clic en **Configure** para especificar los grupos de usuarios a los que se les envía la alerta.



Captura de pantalla 100: Opciones de Digest Report: Ficha Details

5. Haga clic en la ficha **Details** para seleccionar o anular la selección de los elementos de contenido de informe que desee incluir en el informe de resumen.
6. Seleccione la frecuencia de envío del informe entre **Daily**, **Weekly** o **Monthly**.
7. Haga clic en **Apply** y en **OK**.

11 Administración del back-end de base de datos

En este capítulo, se proporciona información relacionada con la administración y el mantenimiento de la base de datos donde se almacenan los datos recopilados por GFI EndPointSecurity. Después de instalar GFI EndPointSecurity, puede elegir lo siguiente:

- Descargar e instalar una instancia de Microsoft SQL Server Express Edition y crear automáticamente una base de datos para GFI EndPointSecurity. Esto se puede realizar a través del **Quick Start wizard**.
- Conectarse a una instancia de Microsoft SQL Server disponible y conectarse a una base de datos existente o crear una nueva. Esto se puede realizar a través del **Quick Start wizard** o de las subfichas **General Status** u **Options**.

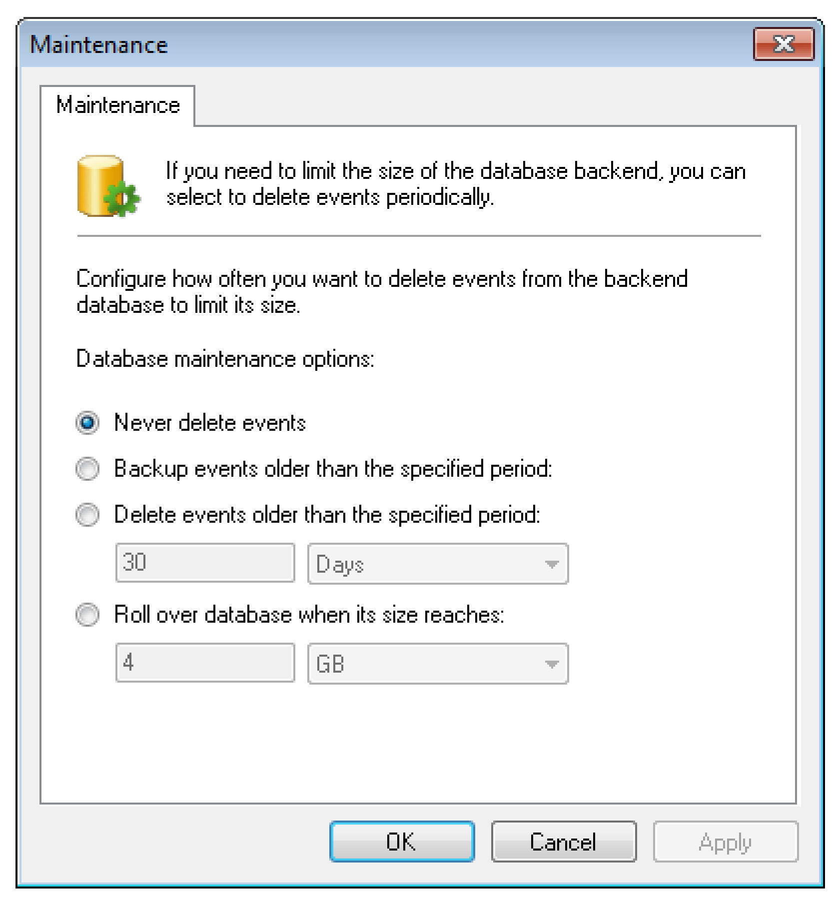
Temas de este capítulo

11.1 Mantenimiento del back-end de base de datos

El mantenimiento periódico de la base de datos es fundamental para evitar que el tamaño del back-end de base de datos aumente demasiado. GFI EndPointSecurity le ofrece la facilidad de configurar parámetros que mantienen automáticamente el back-end de base de datos.

Para configurar el mantenimiento del back-end de base de datos:

1. Haga clic en la ficha **Configuration**, subficha > **Options**.
2. En **Configure**, seleccione **Database Backend**.
3. En el panel derecho, haga clic en **Database maintenance**.



Captura de pantalla 101: Opciones de mantenimiento

4. En el cuadro de diálogo **Maintenance**, configure la frecuencia con la que se eliminarán los eventos del back-end de base de datos. Seleccione entre las opciones que se describen a continuación:

Tabla 17: Opciones de mantenimiento de la base de datos

Opción	Descripción
Never delete events	Mantiene todos los eventos en el back-end de base de datos, sin eliminar los antiguos. **Nota** Asegúrese de que se realice una eliminación manual de los registros antiguos para evitar caídas en el rendimiento de GFI EndPointSecurity.
Backup events older than the specified period	Seleccione esta opción y especifique la antigüedad que deben tener los eventos para que se les realice una copia de seguridad en una base de datos independiente.
Delete events older than the specified period	Seleccione esta opción y especifique la antigüedad que deben tener los eventos para que se los elimine.
Roll over database when its size reaches	Especifique el tamaño máximo que puede tener una base de datos antes de que GFI EndPointSecurity pase automáticamente a una base de datos nueva.

5. Haga clic en **Apply** y en **OK**.



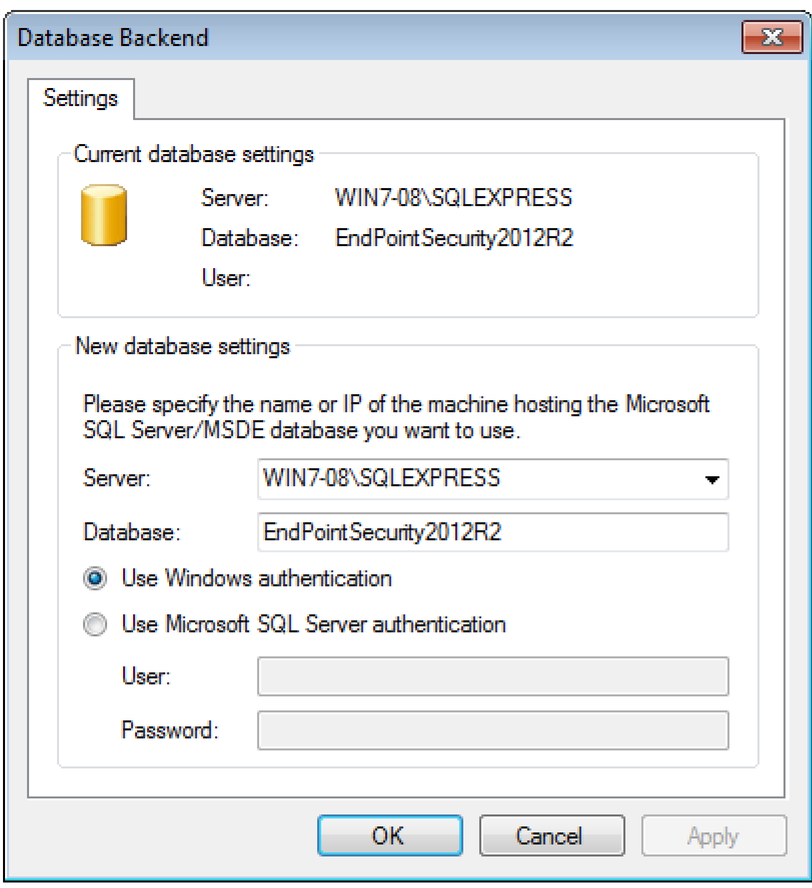
Nota

Dado que Microsoft SQL Express 2005 tiene un límite de tamaño de base de datos de 4 GB y Microsoft SQL Express 2008 R2 tiene un límite de base de datos de 10 GB, se recomienda usar la opción Roll over database. Para obtener más información sobre las especificaciones del motor de Microsoft SQL Server Edition, consulte http://go.gfi.com/?pageid=ESEC_SqlSpecs.

11.2 Uso de una instancia de SQL Server existente

Para conectar una instancia de SQL Server existente:

1. Haga clic en la ficha **Configuration**, subficha > **Options**.
2. En **Configure**, seleccione **Database Backend**.
3. En el panel derecho, haga clic en **Change database backend**.



Captura de pantalla 102: Cambio del back-end de base de datos

4. En el menú desplegable **Server**, seleccione el servidor de SQL Server que desee usar.
5. Especifique el nombre de la base de datos en el cuadro de texto **Database**.
6. Seleccione el modo de autenticación y, si es necesario, especifique las credenciales de inicio de sesión.
7. Haga clic en **Apply** y en **OK**.

12 Opciones de alerta

En este capítulo, se proporciona información acerca de la configuración de las opciones de alerta y los destinatarios de alertas de GFI EndPointSecurity. Las alertas son una parte crucial del funcionamiento de GFI EndPointSecurity que lo ayudan a tomar medidas correctivas en cuanto se detecta una amenaza.

Temas de este capítulo

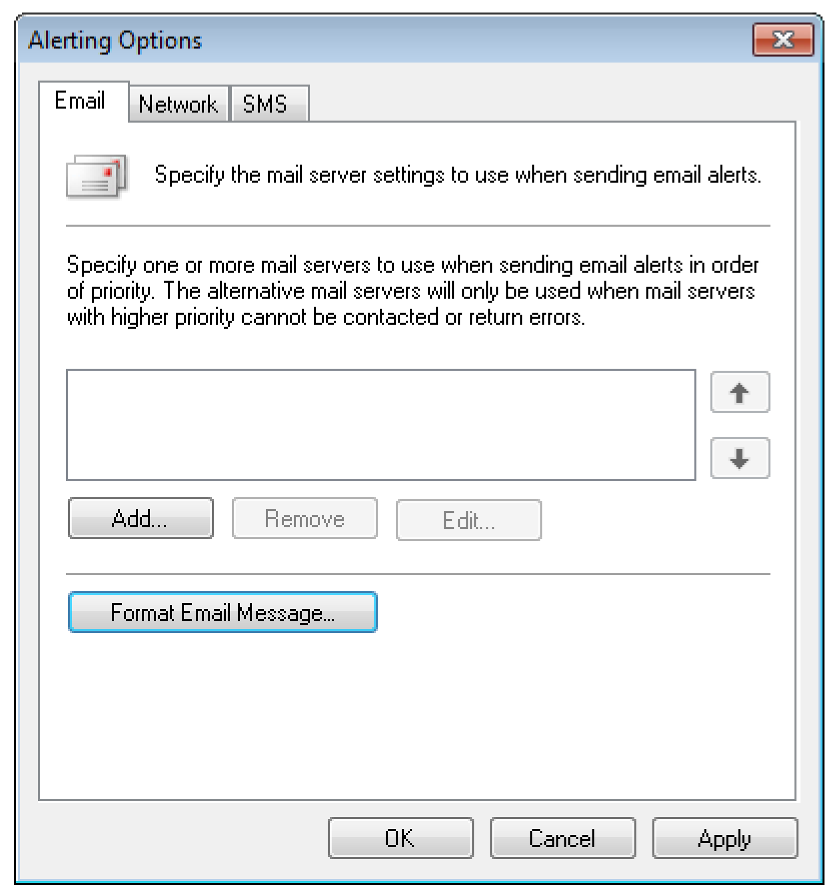
12.1 Configuración de opciones de alerta

GFI EndPointSecurity le permite configurar las siguientes opciones de alerta:

- La configuración de servidor de correo, los detalles del remitente y el mensaje de correo electrónico que se usan al enviar alertas de correo electrónico
- El mensaje de red que se usa al enviar alertas de red
- La puerta de enlace SMS y el mensaje SMS que se usan al enviar alertas por SMS.

Para configurar opciones de alerta:

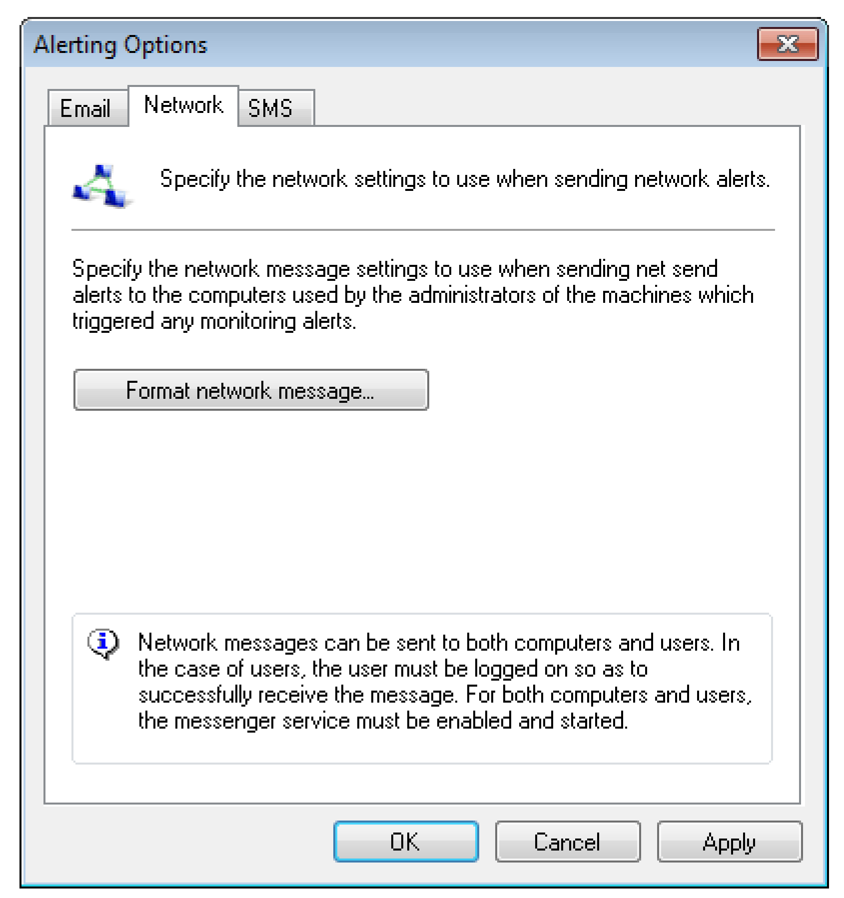
1. Haga clic en la ficha **Configuration**, subficha > **Options**.
2. En **Configure**, haga clic con el botón secundario en el nodo **Alerting Options** y seleccione **Edit alerting options...**.



Captura de pantalla 103: Opciones de alerta: Ficha Email

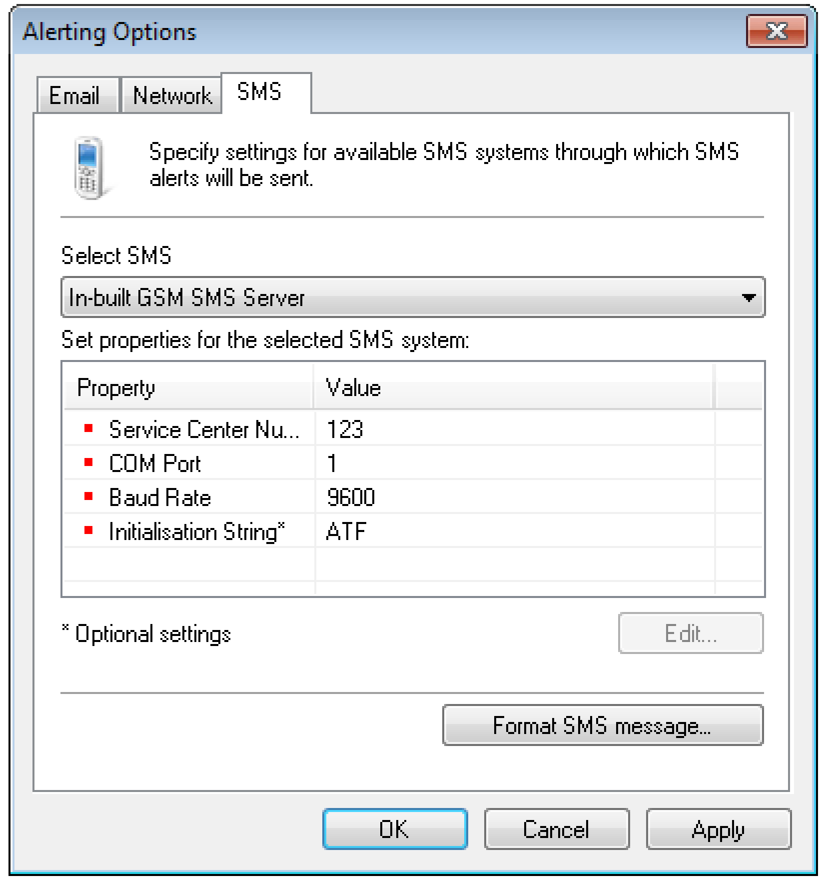
3. En la ficha **Email**, haga clic en **Add...** para especificar su configuración de servidor de correo. Haga clic en **OK** para cerrar el cuadro de diálogo **Mailserver properties**.

4. Para editar el mensaje de correo electrónico, haga clic en **Format Email Message...**, modifique los campos **Subject** y **Message** según se requiera, y haga clic en **Save**.



Captura de pantalla 104: Opciones de alerta: Ficha Network

5. Haga clic en la ficha **Network > Format network message…** para editar el mensaje de red. Haga clic en **Save**.



Captura de pantalla 105: Opciones de alerta: Ficha SMS

6. Haga clic en la ficha **SMS** y, desde el menú desplegable **Select SMS**, seleccione la puerta de enlace SMS que desee usar. Entre los sistemas de SMS admitidos se incluyen:

- In-built GSM SMS Server
- Puerta de enlace SMS GFI FaxMaker
- Servicio de Clickatell Email to SMS Gateway
- Puerta de enlace SMS genérica

7. En el área **Set properties for the selected SMS system**, resalte la propiedad que desee configurar y haga clic en **Edit**. Repita este paso para cada propiedad del sistema de SMS que desee modificar.
8. Haga clic en **Format SMS message...** para modificar los campos Subject y Message según se requiera. Haga clic en **Save**.
9. Haga clic en **OK**.

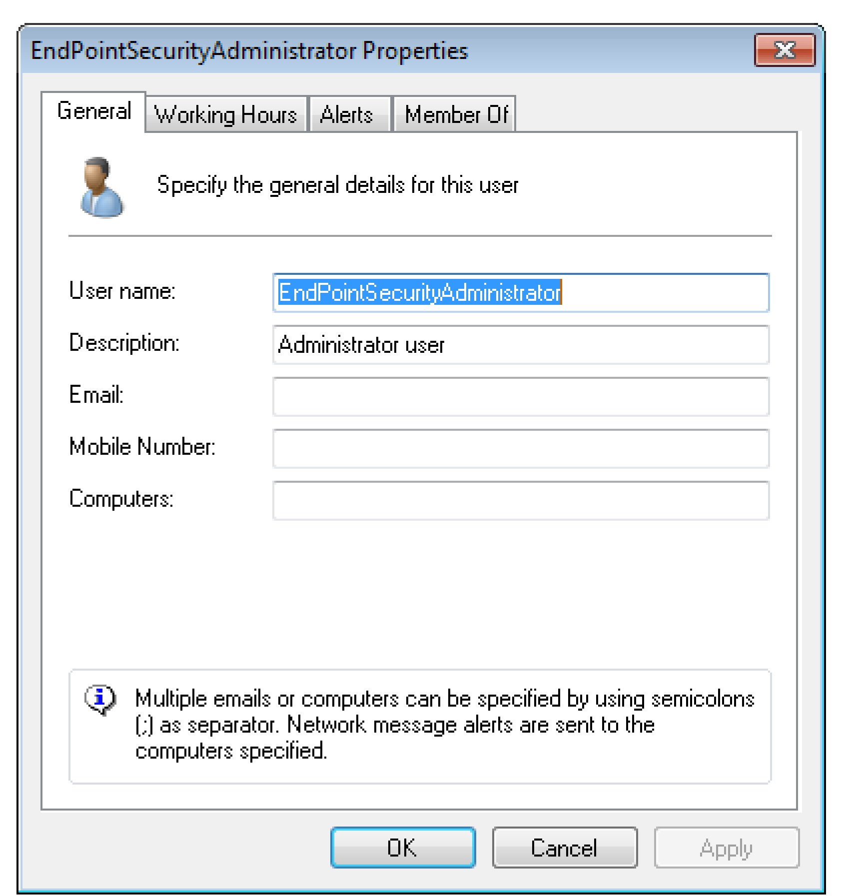
12.2 Configuración de la cuenta del administrador de alertas

GFI EndPointSecurity le permite configurar cuentas de perfil para contener los detalles de contacto de los usuarios que desea que reciban alertas por correo electrónico, mensajes de red y mensajes SMS. Después de la instalación, GFI EndPointSecurity crea automáticamente una cuenta de administrador de alertas. Los administradores de alertas no son usuarios o grupos de usuarios de Active Directory (AD).

De forma predeterminada, GFI EndPointSecurity crea automáticamente la cuenta de EndPointSecurityAdministrator (con fines de alertas) después de la instalación y lo establece como miembro del grupo de notificación de EndPointSecurityAdministrators.

Para configurar la cuenta de GFI EndPointSecurityAdministrator:

1. Haga clic en la ficha **Configuration**, subficha > **Options**.
2. En **Configure**, haga clic en el subnodo **Alerting Options > Users**.
3. En el panel derecho, haga clic con el botón secundario en **EndPointSecurityAdministrator** y seleccione **Properties**.



Captura de pantalla 106: Opciones de propiedades de EndPointSecurityAdministrator: Ficha General

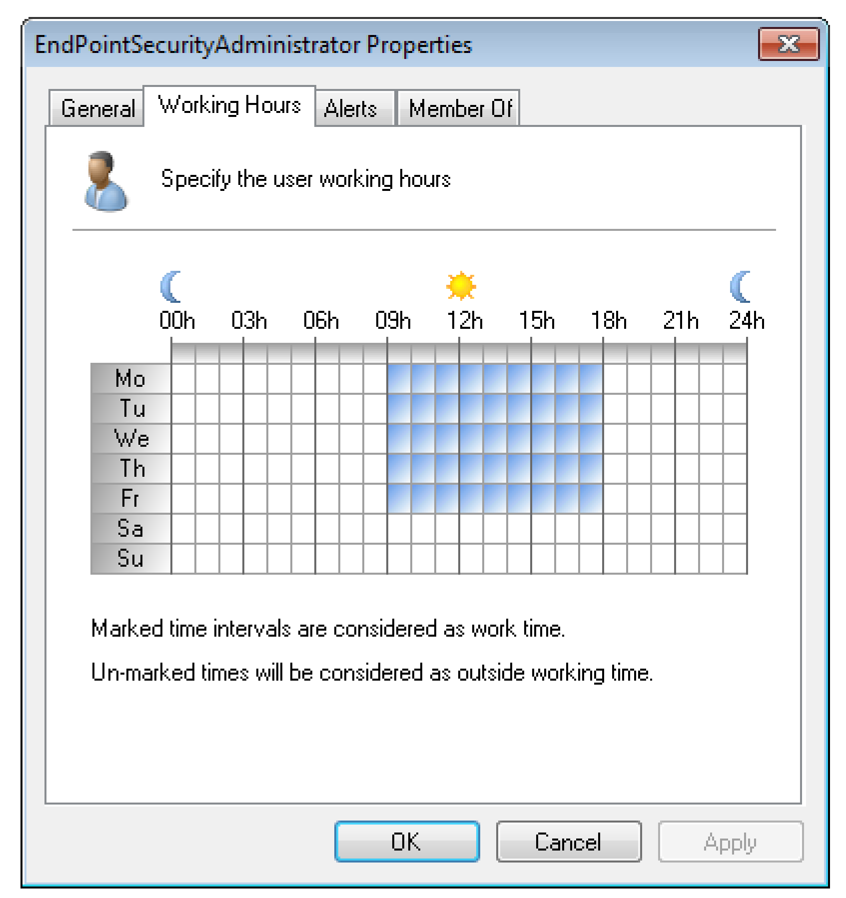
4. En la ficha General, escriba los siguientes detalles:

- Nombre del usuario de la cuenta
- Descripción de la cuenta
- Dirección de correo electrónico
- Número de teléfono móvil
- Equipos (los mensajes de red se envían a los equipos especificados).



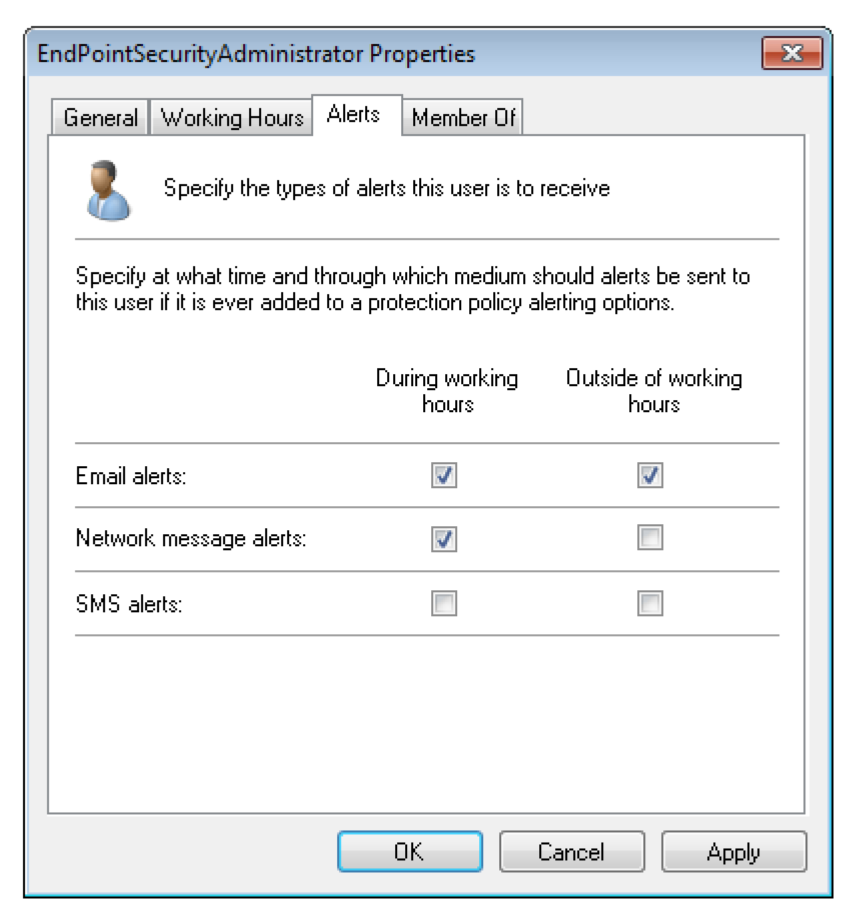
Nota

Pueden especificarse más de una dirección de correo electrónico y más de un nombre de equipo/dirección IP. Separe las entradas con puntos y comas (;).



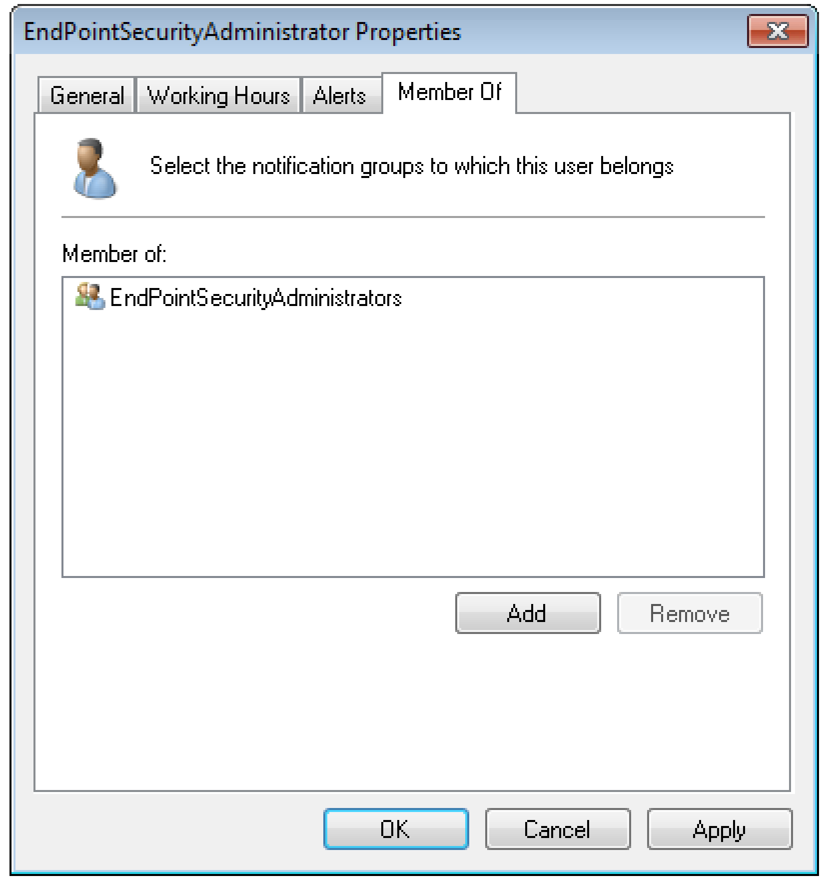
Captura de pantalla 107: Opciones de propiedades de EndPointSecurityAdministrator: Ficha Working Hours

5. Haga clic en la ficha **Working Hours** y marque las horas de trabajo habituales del usuario. Los intervalos de tiempo marcados se consideran horas de trabajo.



Captura de pantalla 108: Opciones de propiedades de EndPointSecurityAdministrator: Ficha Alerts

6. Haga clic en la ficha **Alerts** y seleccione las alertas que desee que se envíen y la hora a la que se deben enviar.



Captura de pantalla 109: Opciones de propiedades de EndPointSecurityAdministrator: Ficha Member Of

7. Haga clic en la ficha **Member Of** y haga clic en **Add** para agregar el usuario al grupo de notificación.
8. Haga clic en **Apply** y en **OK**.

12.3 Configuración de destinatarios de alertas

GFI EndPointSecurity le permite configurar otras cuentas de perfil (aparte de la cuenta de administrador de GFI EndPointSecurity predeterminada) para contener los detalles de contacto de los usuarios que desea que reciban alertas por correo electrónico, mensajes de red y mensajes SMS.

Los destinatarios de alertas no son usuarios o grupos de usuarios de Active Directory (AD), sino que son cuentas de perfil creadas por GFI EndPointSecurity para contener los detalles de contacto de los usuarios a los que se destinan las alertas.

» Creación de destinatarios de alertas
» Edición de propiedades de destinatarios de alertas
» Eliminación de destinatarios de alertas

12.3.1 Creación de destinatarios de alertas

Para crear un nuevo destinatario de alertas:

1. Haga clic en la ficha **Configuration**, subficha > **Options**.
2. En **Configure**, haga clic en el subnodo **Alerting Options** > **Users**.
3. En el panel izquierdo, haga clic en **Create user...**.

4. Para obtener más información sobre cómo establecer la configuración para crear un nuevo destinatario, consulte Configuración de la cuenta del administrador de alertas.

12.3.2 Edición de propiedades de destinatarios de alertas

Para editar las propiedades de los destinatarios de alertas:

1. Haga clic en la ficha **Configuration**, subficha > **Options**.
2. En **Configure**, haga clic en el subnodo **Alerting Options > Users**.
3. En el panel derecho, haga clic con el botón secundario en el usuario que desee editar y seleccione **Properties**.
4. Para obtener más información sobre cómo establecer la configuración para editar un destinatario, consulte Configuración de la cuenta del administrador de alertas.

12.3.3 Eliminación de destinatarios de alertas

Para eliminar un destinatario de alertas:

1. Haga clic en la ficha **Configuration**, subficha > **Options**.
2. En **Configure**, haga clic en el subnodo **Alerting Options > Users**.
3. En el panel derecho, haga clic con el botón secundario en el usuario que desee eliminar y seleccione **Delete**.
4. Haga clic en **Yes** para confirmar la eliminación.

12.4 Configuración de grupos de destinatarios de las alertas

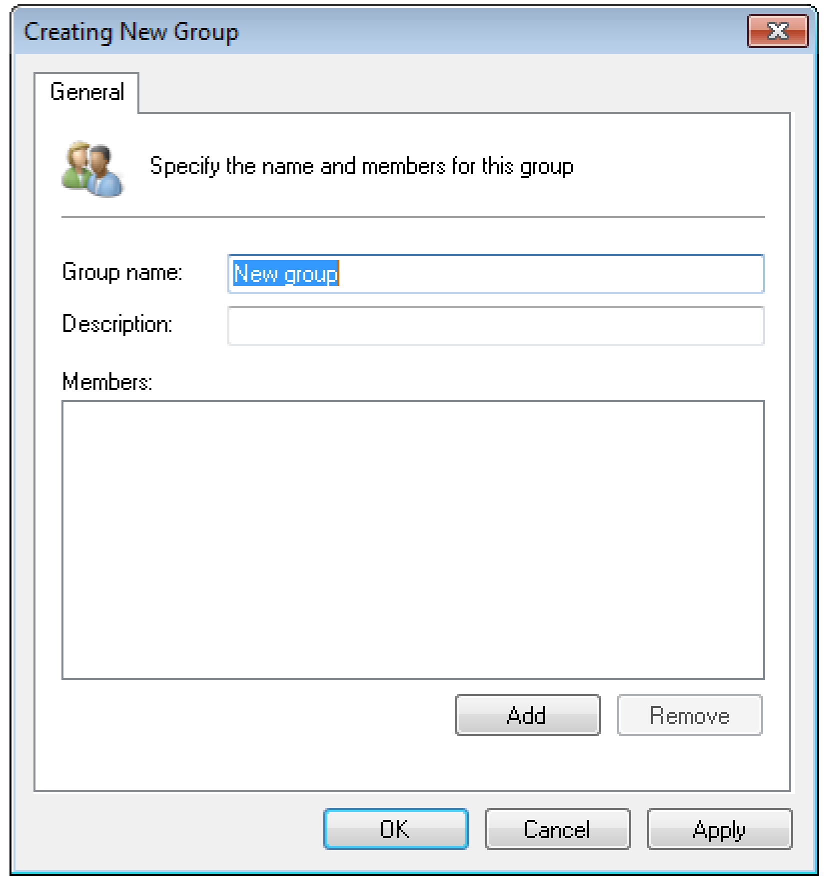
GFI EndPointSecurity le permite organizar sus destinatarios de alertas en grupos, a fin de facilitar su administración.

- Creación de grupos de destinatarios de alertas
- Edición de propiedades de grupos de destinatarios de alertas
- Eliminación de grupos de destinatarios de alertas

12.4.1 Creación de grupos de destinatarios de alertas

Para crear un nuevo grupo de destinatarios de alertas:

1. Haga clic en la ficha **Configuration**, subficha > **Options**.
2. Haga clic en el subnodo **Alerting Options > Groups**.
3. En el panel izquierdo, haga clic en **Create group…**.



Captura de pantalla 110: Creación de opciones de grupo nuevo

4. En el cuadro de diálogo **Creating New Group**, escriba el nombre de grupo y una descripción opcional.

5. Haga clic en **Add** para seleccionar los usuarios que pertenezcan a este grupo de notificación y haga clic en **OK**.

12.4.2 Edición de propiedades de grupos de destinatarios de alertas

Para editar las propiedades de un grupo de destinatarios de alertas:

1. Haga clic en la ficha **Configuration**, subficha > **Options**.

2. Haga clic en el subnodo **Alerting Options > Groups**.

3. En el panel derecho, haga clic con el botón secundario en el grupo que desee editar y seleccione **Properties**.

4. Para obtener más información sobre cómo editar la configuración de grupos, consulte Creación de grupos de destinatarios de alertas.

12.4.3 Eliminación de grupos de destinatarios de alertas

Para eliminar un grupo de destinatarios de alertas:

1. Haga clic en la ficha **Configuration**, subficha > **Options**.

2. Haga clic en el subnodo **Alerting Options > Groups**.

3. En el panel derecho, haga clic con el botón secundario en el grupo que desee eliminar y seleccione **Delete**.

4. Haga clic en **Yes** para confirmar la eliminación del grupo.

13 Configuración de GFI EndPointSecurity

GFI EndPointSecurity le permite configurar los equipos en los cuales desea instalar actualizaciones y mostrar mensajes de usuarios.

Temas de este capítulo

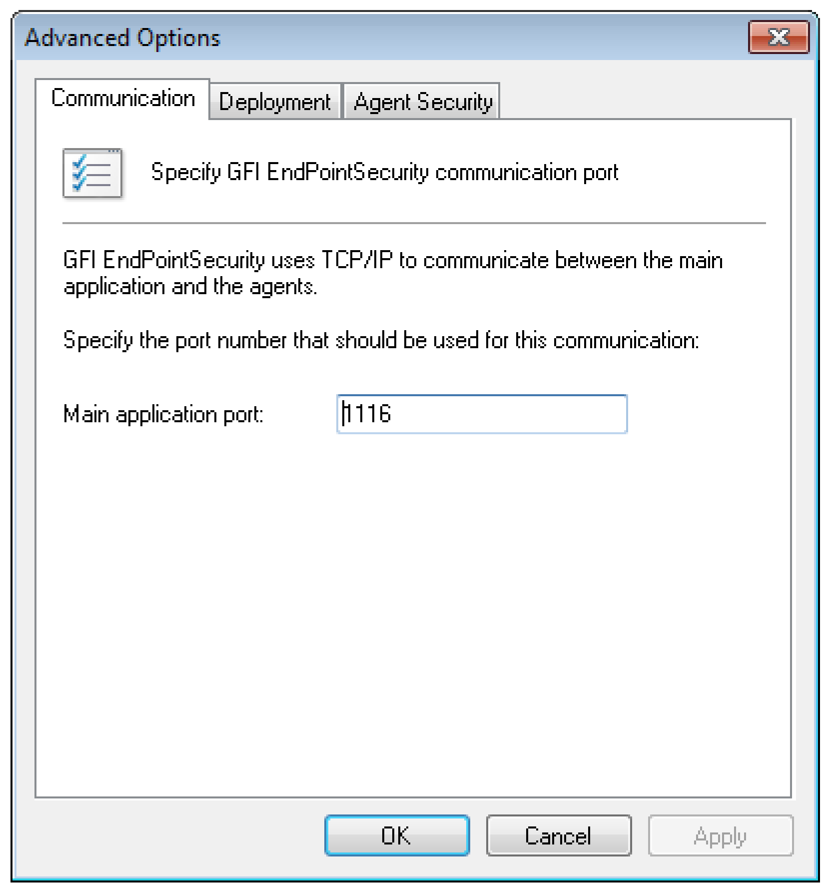
13.1 Configuración de opciones avanzadas

GFI EndPointSecurity le permite configurar las siguientes opciones avanzadas del agente:

- Puerto TCP/IP de comunicación principal
- Opciones de implementación
- Contraseña de control de agentes.

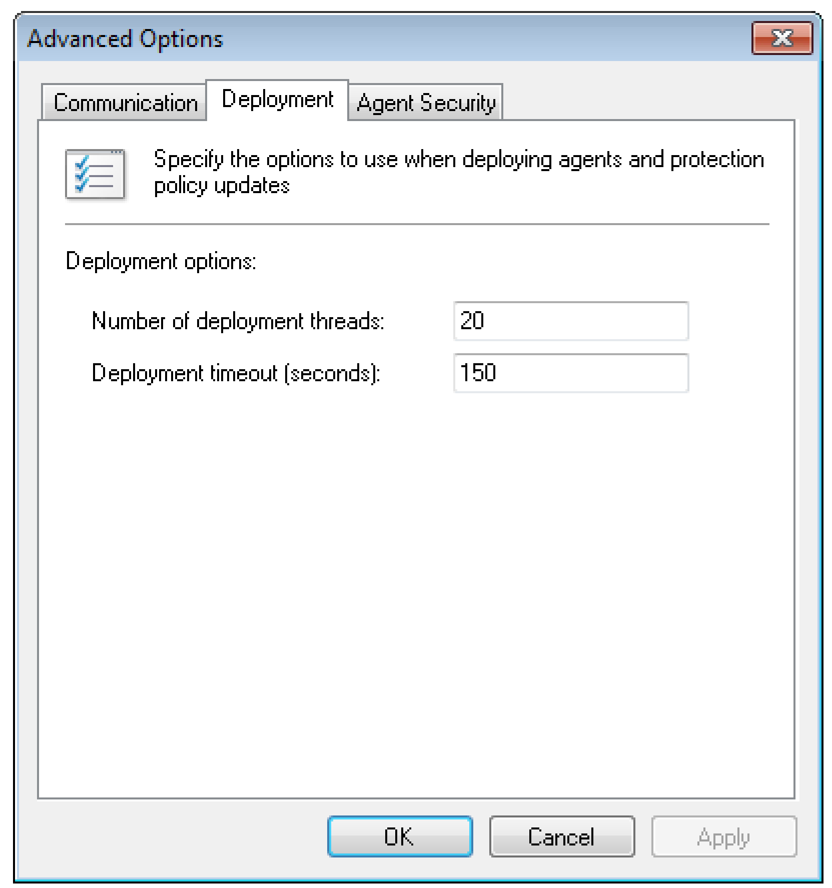
Para configurar opciones avanzadas:

1. Haga clic en la ficha **Configuration**, subficha > **Options**.
2. En **Configure**, haga clic con el botón secundario en el nodo **Advanced Options** y seleccione **Modify advanced options...**.



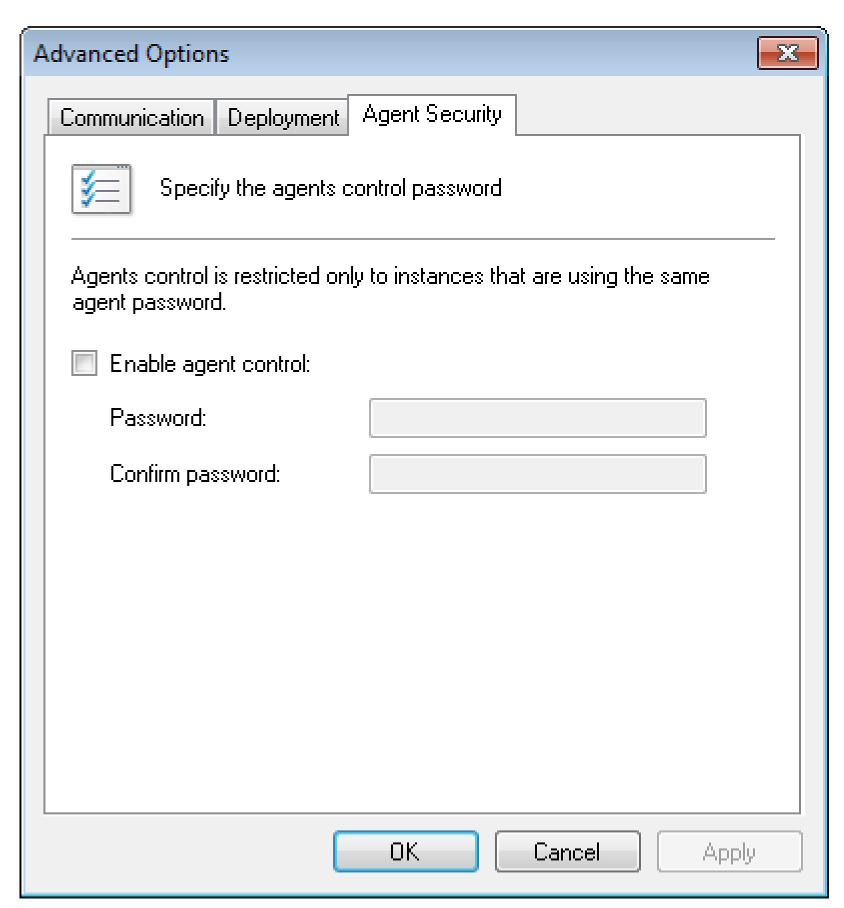
Captura de pantalla 111: Opciones avanzadas: Ficha Communication

3. En la ficha **Communication**, escriba el número de puerto TCP/IP necesario para la comunicación entre GFI EndPointSecurity y los agentes de GFI EndPointSecurity. De forma predeterminada, se especifica el puerto **1116**.



Captura de pantalla 112: Opciones avanzadas: Ficha Deployment

4. Haga clic en la ficha **Deployment** y escriba los valores de **Number of deployment threads** y **Deployment timeout (seconds)** obligatorios.



Captura de pantalla 113: Opciones avanzadas: Ficha Agent Security

5. Haga clic en la ficha **Agent Security** y seleccione o anule la selección de **Enable agent control**. Use esta opción para asignar credenciales de inicio de sesión particulares a todos los agentes de GFI EndPointSecurity implementados en la red.

6. Haga clic en **Apply** y en **OK**.

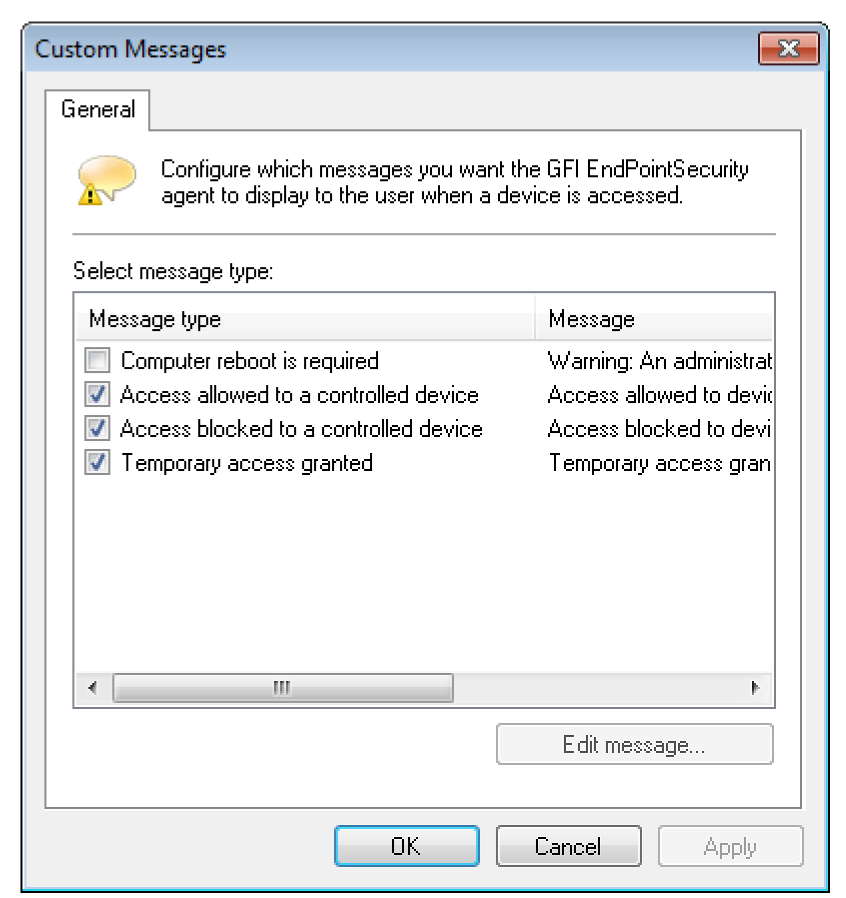
13.2 Configuración de mensajes de usuarios

GFI EndPointSecurity le permite personalizar los mensajes que muestran los agentes de GFI EndPointSecurity en los equipos de destino cuando se accede a los dispositivos.

Para personalizar los mensajes de usuarios:

1. Haga clic en la ficha **Configuration**, subficha > **Options**.

2. En Configure, haga clic con el botón secundario en Custom Messages y seleccione Customize user messages.



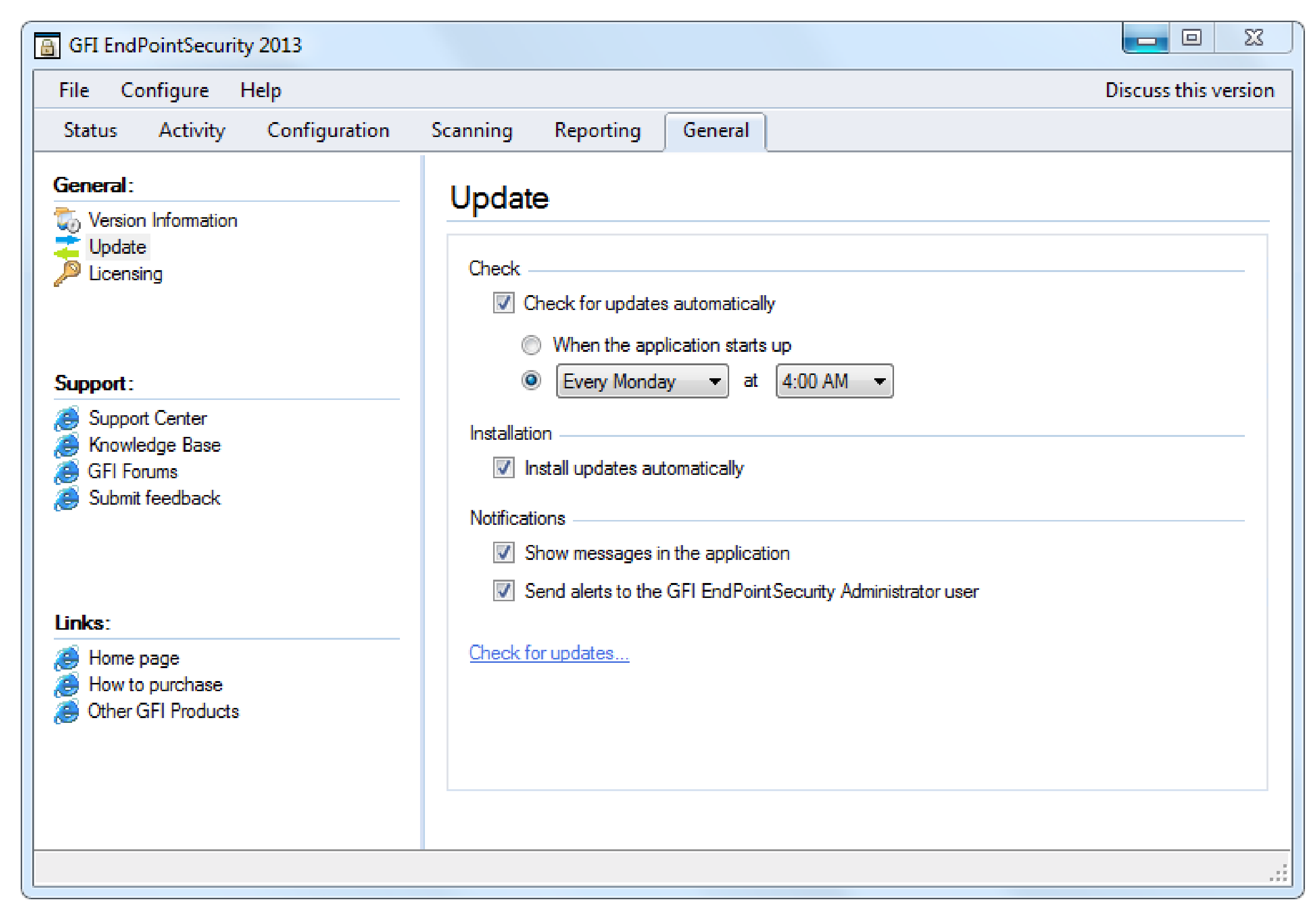
Captura de pantalla 114: Opciones del cuadro de diálogo Custom Messages

3. Seleccione o anule la selección de los tipos de mensajes que desee personalizar.
4. Para cada tipo de mensaje seleccionado, haga clic en **Edit message…**, modifique el texto según se requiera, y haga clic en **Save**. Repita este paso para cada mensaje que desee modificar.
5. Haga clic en **Apply** y en **OK**.

13.3 Configuración de actualizaciones de GFI EndPointSecurity

GFI EndPointSecurity se puede configurar para que descargue e instale actualizaciones automáticamente con una programación o en el inicio. Para configurar actualizaciones:

1. Haga clic en la ficha **General**.
2. En el panel izquierdo, haga clic en **Updates**.



Captura de pantalla 115: Ficha General: Actualizaciones

3. En el panel derecho, configure las opciones que se describen a continuación:

Tabla 18: Opciones de actualización

Opción	Descripción
Check for updates automatically	Se conecta a los servidores de actualizaciones de GFI y descarga actualizaciones del producto automáticamente. Seleccione "When the application starts up" o especifique un día y una hora para comprobar y descargar actualizaciones.
Install updates automatically	Si se encuentra una actualización, GFI EndPointSecurity la descargará y la instalará automáticamente.
Show messages in the application	Si se encuentra y se instala una actualización, se muestra un mensaje en la aplicación GFI EndPointSecurity.
Send alerts to the GFI EndPointSecurity Administrator user	Una vez que se descarga e instala una actualización, se envía un mensaje de correo electrónico al administrador de GFI EndPointSecurity. Para obtener más información, consulte Configuración de la cuenta del administrador de alertas (página 134).
Check for updates	Haga clic en el vínculo para ejecutar al instante el motor de actualizaciones de GFI EndPointSecurity, descargar las actualizaciones faltantes e instalarlas.

14 Varios

En el capítulo sobre varios, se recopila toda la demás información que no se relaciona con la configuración inicial de GFI EndPointSecurity.

Temas de este capítulo

14.1 Licencias del producto

Después de instalar GFI EndPointSecurity, puede introducir su clave de licencia sin volver a instalar ni configurar la aplicación.

Para introducir la clave de licencia:

1. Haga clic en la ficha **General**.
2. En el panel izquierdo, seleccione **Licensing**.

Captura de pantalla 116: Edición de la clave de licencia

3. En el panel derecho, haga clic en **Edit…**.
4. En el cuadro de texto **License Key**, escriba la clave de licencia proporcionada por GFI Software Ltd.
5. Haga clic en **OK** para aplicar la clave de licencia.

14.2 Desinstalación de GFI EndPointSecurity

GFI EndPointSecurity le permite desinstalar fácilmente los agentes de GFI EndPointSecurity y la aplicación GFI EndPointSecurity.

En este capítulo, se abarcan los siguientes temas:

» Desinstalación de agentes de GFI EndpointSecurity

» Desinstalación de la aplicación GFI EndpointSecurity



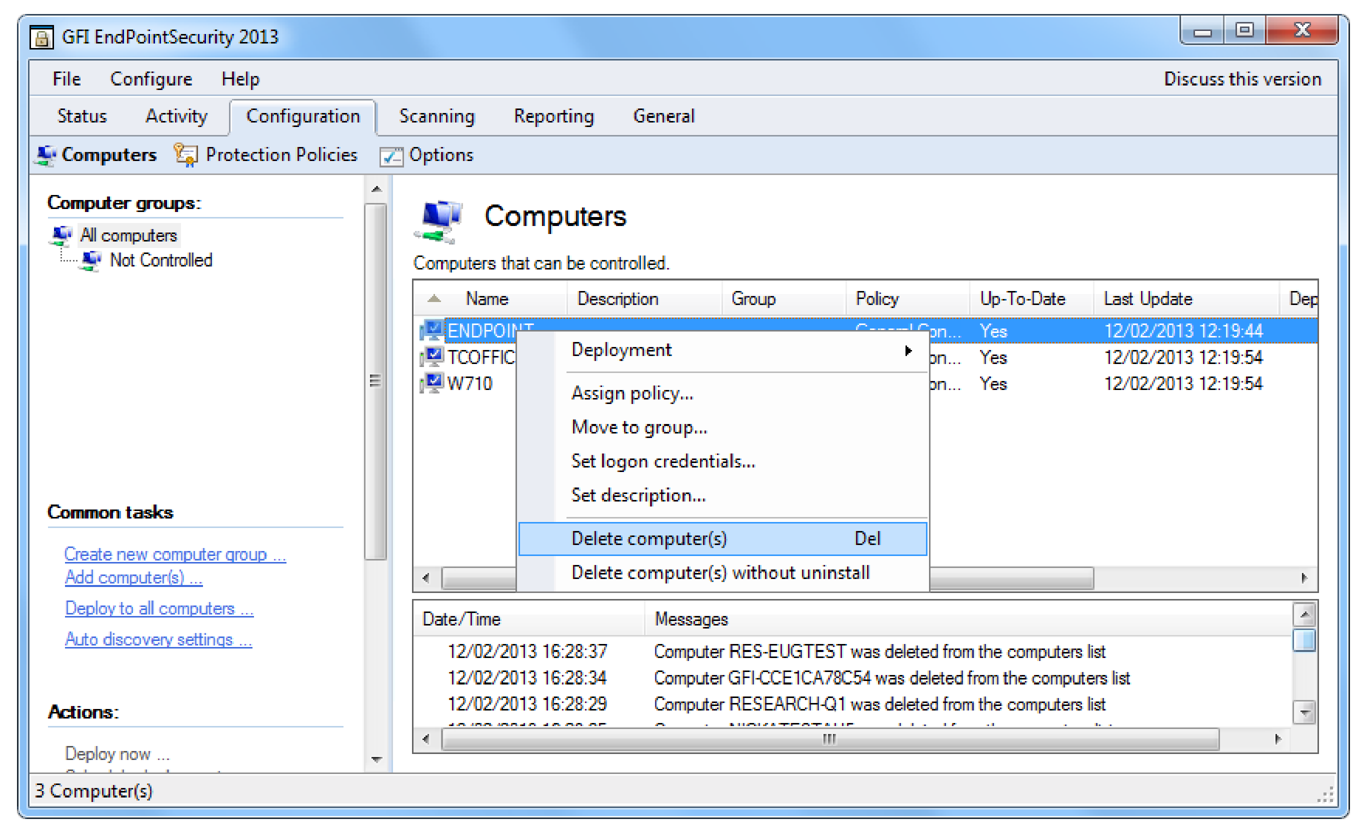
Advertencia

Los agentes de GFI EndPointSecurity no se desinstalan automáticamente durante la desinstalación de la aplicación GFI EndPointSecurity. Es mejor desinstalar primero los agentes de GFI EndPointSecurity y después la aplicación GFI EndPointSecurity.

14.2.1 Desinstalación de agentes de GFI EndPointSecurity

Para desinstalar un agente de GFI EndPointSecurity:

1. En la consola de administración de GFI EndPointSecurity, haga clic en la ficha **Configuration**.
2. Haga clic en la subficha **Computers**.



Captura de pantalla 117: Subficha Computers: Delete computer(s)

3. En el panel derecho, haga clic con el botón secundario en el equipo de destino que desee desinstalar y seleccione:

Deleting Computer(s)	
Deleting computer(s) - **with** uninstallation	GFI EndPointSecurity implementará actualizaciones de la directiva de protección y desinstalará el agente.
Deleting computer(s) - **without** uninstallation	GFI EndPointSecurity implementará actualizaciones de la directiva de protección y eliminará la entrada del equipo relevante de la lista Computers. Sin embargo, dejará el agente instalado en el equipo de destino. Esto resulta útil cuando el equipo de destino se ha eliminado de la red y la aplicación GFI EndPointSecurity no puede conectarse con él para desinstalar el agente.

4. Haga clic en **Yes** para confirmar la eliminación del equipo seleccionado de la lista.

5. En el panel derecho, haga clic en el mensaje de advertencia superior para implementar las actualizaciones de la directiva de protección. La vista debe cambiar automáticamente a **Status > Deployment**.

Captura de pantalla 118: Subficha Deployment

6. En el área **Deployment History**, confirme que la desinstalación del equipo de destino haya finalizado correctamente.

14.2.2 Desinstalación de la aplicación GFI EndPointSecurity

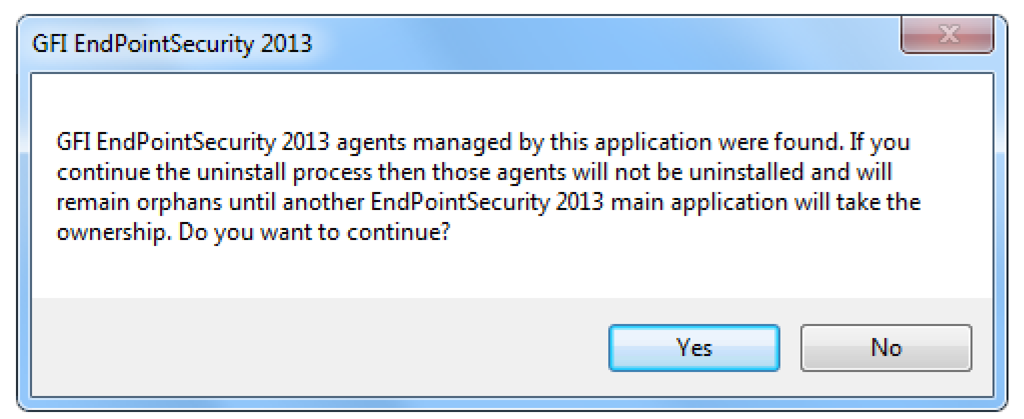
Para desinstalar la aplicación GFI EndPointSecurity:



Nota

Ejecute el desinstalador como usuario con privilegios administrativos en el equipo.

1. En el **Panel de control de Microsoft Windows**, seleccione **Agregar o quitar programas** o **Programas y características**.
2. Seleccione GFI EndPointSecurity.
3. Haga clic en **Change** para iniciar la desinstalación de la aplicación GFI EndPointSecurity.
4. Haga clic en **Next** en la pantalla de bienvenida para continuar la desinstalación.



Captura de pantalla 119: Mensaje de información de desinstalación



Nota

Si todavía hay agentes instalados, se muestra un cuadro de diálogo de información donde se le pregunta si desea continuar (los agentes permanecerán instalados y huérfanos) o detener el proceso de desinstalación. Para obtener más información acerca de la desinstalación de agentes, consulte la sección Desinstalación de agentes de GFI EndPointSecurity de este capítulo.

5. Seleccione la opción **Uninstall without deleting configuration files** o **Complete uninstall** y haga clic en **Next** para continuar.
6. Cuando se complete, haga clic en **Finish** para finalizar la desinstalación.

14.3 Información de versión del producto

GFI Software Ltd. lanza actualizaciones del producto que pueden descargarse manual o automáticamente del sitio web de GFI.

Para comprobar si hay una versión más reciente de GFI EndPointSecurity disponible para descargar:

1. Haga clic en la ficha **General**.
2. En el panel izquierdo, seleccione **Version Information**.
3. En el panel derecho, haga clic en **Check for newer version** para comprobar manualmente si hay una versión más reciente de GFI EndPointSecurity disponible. Como alternativa, seleccione **Check for newer version at startup** para comprobar automáticamente si hay una versión más reciente de GFI EndPointSecurity disponible para descargar cada vez que se inicie la consola de administración.

15 Solución de problemas y asistencia técnica

Este capítulo explica cómo resolver los problemas detectados durante la instalación de GFI EndPointSecurity. Las principales fuentes de información disponibles para solucionar estos problemas son:

Esta sección y el resto de la Guía del administrador de GFI EndPointSecurity contiene soluciones a todos los posibles problemas que puede detectar. Si no puede resolver un problema, comuníquese con el Servicio técnico de GFI para obtener más ayuda.

Problemas comunes

En la tabla que se incluye a continuación, se muestran los problemas más comunes que puede detectar durante la configuración inicial y el primer uso de GFI EndPointSecurity y una posible solución a cada uno de ellos:

Tabla 19: Solución de problemas: Problemas comunes

Problema	Causa posible	Solución posible
El equipo está desconectado.	La consola de administración de GFI EndPointSecurity hace ping en el equipo de destino en la implementación para determinar si está en línea y, de lo contrario, se muestra este mensaje.	Si un equipo de destino está desconectado, la implementación de la directiva de protección relevante se reprogramará para una hora más tarde. GFI EndPointSecurity sigue intentando implementar esa directiva cada hora, hasta que el equipo de destino se vuelve a conectar. Asegúrese de que el equipo de destino esté encendido y conectado a la red.
Error al conectarse con el registro remoto (error).	GFI EndPointSecurity no pudo extraer los datos del registro del equipo de destino.	Asegúrese de que la configuración del cortafuegos habilite la comunicación entre los equipos de destino y el servidor de GFI EndPointSecurity. Para obtener más información, consulte Requisitos del sistema.
Error al recopilar la información necesaria (error).	GFI EndPointSecurity no pudo extraer los datos relacionados con la versión del equipo de destino (versión del sistema operativo y versión del agente de GFI EndPointSecurity).	Para obtener más detalles acerca de la causa del error y una posible solución, consulte el mensaje de error del sistema dentro de los paréntesis.
Error al crear los archivos de instalación necesarios (error).	GFI EndPointSecurity no pudo agregar los archivos de configuración necesarios dentro del archivo de implementación (archivo de instalación .msi) del agente de GFI EndPointSecurity. Este error ocurre antes de que el archivo de implementación se copie en el equipo de destino.	Para obtener más detalles acerca de la causa del error y una posible solución, consulte el mensaje de error del sistema dentro de los paréntesis.
Error al copiar los archivos en el equipo remoto (error).	GFI EndPointSecurity no pudo copiar el archivo de implementación (archivo de instalación .msi) en el equipo remoto. Una posible causa puede ser que el recurso compartido administrativo (C$) que utiliza GFI EndPointSecurity para conectarse al equipo de destino esté deshabilitado.	Para obtener más detalles acerca de la causa del error y una posible solución, consulte el mensaje de error del sistema dentro de los paréntesis. Para obtener más información acerca de la conectividad de red y los permisos de seguridad, consulte: http://kb.gfi.com/articles/SkyNet_Article/KBID003754?retURL=%2Fapex%2FSupportHome&popup=true

Problema	Causa posible	Solución posible
Tiempo de espera	La implementación del agente en el equipo de destino está tardando demasiado en finalizar o está bloqueada.	Intente volver a implementar el agente de GFI EndPointSecurity.
Error en la instalación del servicio de implementación (error).	El servicio que está en ejecución en el equipo de destino no pudo instalar o desinstalar el agente de GFI EndPointSecurity.	Para obtener más detalles acerca de la causa del error y una posible solución, consulte el mensaje de error del sistema dentro de los paréntesis.
Error en la instalación.	Se completó la instalación del agente de GFI EndPointSecurity, pero no está marcado como instalado dentro del registro. Los números de versión y compilación del agente de GFI EndPointSecurity no son los mismos que los de la consola de administración de GFI EndPointSecurity.	Para obtener más detalles acerca de la causa del error y una posible solución, consulte los archivos de registro de instalación del agente en el equipo de destino en: **%windir%\EndPointSecurity**.
Error en la desinstalación.	Se completó la desinstalación del agente de GFI EndPointSecurity, pero no está marcado como desinstalado dentro del registro.	Para obtener más detalles acerca de la causa del error y una posible solución, consulte los archivos de registro de instalación del agente en el equipo de destino en: **%windir%\EndPointSecurity**.
Se produjo un error en la operación debido a una excepción desconocida.	GFI EndPointSecurity ha detectado un error inesperado.	Utilice el asistente para el solucionador de problemas para comunicarse con el equipo de asistencia técnica de GFI. Para abrir el asistente para el solucionador de problemas, vaya a **Inicio** > **Programas** > **GFI EndPointSecurity 2013** > **GFI EndPointSecurity 2013 Troubleshooter**.

Uso de GFI EndPointSecurity Troubleshooter

Para usar el solucionador de problemas proporcionado por GFI EndPointSecurity:

1. Haga clic en **Inicio** > **Programas** > **GFI EndPointSecurity2013** > **GFI EndPointSecurity2013 Troubleshooter**.
2. Haga clic en **Next** en la pantalla de bienvenida del asistente.

Captura de pantalla 120: Especificación de los detalles de contacto y de compra

3. Especifique sus datos de contacto para que nuestro equipo de soporte pueda comunicarse con usted para obtener más información de análisis. Haga clic en **Next**.

Captura de pantalla 121: Especificación de los detalles del problema y otra información relevante para recrear el problema

4. Especifique el error que se genera y otros datos que podrían ayudar a nuestro equipo de soporte a recrear este problema. Haga clic en **Next**.

Captura de pantalla 122: Recopilación de información del equipo

5. El solucionador de problemas analiza su sistema para obtener información acerca del hardware. Puede agregar manualmente más información en el espacio proporcionado o hacer clic en **Next**.

Captura de pantalla 123: Finalizar el asistente para el solucionador de problemas

6. En esta etapa, el solucionador de problemas crea un paquete con la información recopilada en los pasos anteriores. A continuación, se debe enviar el paquete a nuestro equipo de soporte para que pueda analizar y resolver el problema. Haga clic en los botones que se describen a continuación para ver las opciones de envío:

- **Open Containing Folder**: Permite abrir la carpeta que contiene el paquete generado por el solucionador de problemas de modo que pueda enviarlo manualmente por correo electrónico.
- **Go to GFI Support**: Permite abrir la página de soporte del sitio web de GFI.

7. Haga clic en **Finish**.

GFI SkyNet

GFI mantiene un exhaustivo repositorio de su base de conocimientos, que incluye respuestas a los problemas más habituales. GFI SkyNet tiene siempre la lista más actualizada de preguntas y revisiones de soporte técnico. Si la información de esta guía no soluciona sus problemas, consulte GFI SkyNet; para ello, visite http://kb.gfi.com/.

Foro en la red

La asistencia técnica de usuario a usuario está disponible a través del foro de la red de GFI. Para acceder al foro web, visite: http://forums.gfi.com/.

Solicitar soporte técnico

Si ninguno de los recursos especificados anteriormente le permite solucionar los problemas, póngase en contacto con el equipo de Soporte técnico de GFI rellenando un formulario de solicitud de soporte técnico en línea, o bien de forma telefónica.

- **En línea**: Complete el formulario de solicitud de soporte técnico y siga las instrucciones detalladas que se indican en esta página para enviar su solicitud de soporte técnico en: http://support.gfi.com/supportrequestform.asp.
- **Teléfono**: Para obtener el número de teléfono de soporte técnico correspondiente a su región, visite: http://www.gfi.com/company/contact.htm.



NOTA

Antes de ponerse en contacto con el Centro de soporte técnico, tenga su identificación de cliente a mano. Su ID de cliente es el número de cuenta en línea que se le asigna cuando registra por primera vez sus claves de licencia en el área de clientes de GFI en: http://customers.gfi.com.

Le responderemos en 24 horas, o antes, en función de su huso horario.

Documentación

Si este manual no cumple sus expectativas o si cree que esta documentación se puede mejorar, indíquenoslo enviando un correo electrónico a: documentation@gfi.com.

16 Glosario

A

Acceso temporal

Un período durante el cual los usuarios pueden acceder a los dispositivos y puertos de conexión (cuando normalmente ese acceso está bloqueado) en equipos de destino protegidos durante una duración y un intervalo de tiempo determinados.

Active Directory

Tecnología que proporciona diversos servicios de red, entre los que se incluyen los servicios de directorio similares a LDAP.

Agente de GFI EndPointSecurity

Un servicio del cliente responsable de la implementación y la aplicación de las directivas de protección en los equipos de destino.

Alertas

Un conjunto de notificaciones (alertas por correo electrónico, mensajes de red o mensajes SMS) que se envían a destinatarios de alertas cuando se generan eventos específicos.

Aplicación GFI EndPointSecurity

Aplicación de seguridad del servidor que ayuda a mantener la integridad de datos mediante la prevención del acceso y la transferencia de contenido no autorizados hacia y desde dispositivos y puertos de conexión.

Archivo MSI

Un archivo generado por GFI EndPointSecurity para la implementación posterior con GPO u otras opciones de implementación. Se puede generar para cualquier directiva de protección y contiene todos los parámetros de seguridad relevantes configurados, incluida la configuración de instalación para equipos de destino no protegidos.

Asistente para inicio rápido

Un asistente que lo guía en la configuración de GFI EndPointSecurity con parámetros de configuración personalizados. Se inicia después de que se abre la consola de administración de GFI EndPointSecurity por primera vez y está previsto para el primer uso.

Asistente para la creación de directivas de protección

Un asistente que lo guía en la creación y configuración de directivas de protección nuevas. Los parámetros de configuración incluyen la selección de categorías de dispositivos y puertos para controlar y si desea bloquear o permitir el acceso a ellos. Este asistente también le permite configurar filtros por tipo de archivo, permisos de cifrado y opciones de alerta y registro.

B

Back-end de base de datos

Una base de datos que utiliza GFI EndPointSecurity para realizar un seguimiento de las auditorías de todos los eventos generados por agentes de GFI EndPointSecurity implementados en los equipos de destino.

BitLocker To Go

En Microsoft Windows 7, una función para proteger y cifrar los datos en dispositivos extraíbles.

C

Categoría del dispositivo

Un grupo de periféricos organizados en una categoría.

Cifrado de seguridad

Un conjunto de restricciones configuradas para bloquear o permitir que usuarios o grupos accedan a tipos de archivo específicos almacenados en dispositivos cifrados con BitLocker To Go. Estas restricciones se aplican cuando los dispositivos cifrados se conectan a los equipos de destino abarcados por la directiva de protección.

Consola de administración de GFI EndPointSecurity

La interfaz de usuario de la aplicación del servidor de GFI EndPointSecurity.

Cuenta de administrador de alertas

Una cuenta de destinatario de alerta que GFI EndPointSecurity crea automáticamente después de la instalación.

D

Destinatario de alerta

Una cuenta de perfil de GFI EndPointSecurity para contener los detalles de contacto de los usuarios que desea que reciban alertas por correo electrónico, mensajes de red y mensajes SMS.

Detección automática

Una función de GFI EndPointSecurity para buscar y detectar equipos que se conectaron recientemente a la red en períodos programados configurados.

Directiva de protección

Un conjunto de permisos de puertos de conectividad y acceso a dispositivos que se puede configurar para que se ajuste a las directivas de seguridad de acceso de su compañía.

Dispositivos de interfaz humana (HID)

Una especificación que es parte del estándar de bus serie universal (USB) para una clase de dispositivos periféricos. Estos dispositivos, como mouse, teclado y joystick, les permiten a los usuarios introducir datos o interactuar directamente con el equipo.

E

Equipo de destino

Un equipo protegido con una directiva de protección de GFI EndPointSecurity.

Examen de dispositivos

Una función de GFI EndPointSecurity para buscar todos los dispositivos que están o han estado conectados a los equipos de destino examinados.

F

Filtros por tipo de archivo

Un conjunto de restricciones que se asignan a los usuarios y grupos por tipo de archivo. El filtrado se basa en comprobaciones de extensión de archivo y comprobaciones de firma de tipo de archivo real.

G

GPO

Véase Objetos de directiva de grupo

H

Herramienta GFI EndPointSecurity Temporary Access

Una herramienta que está disponible en los equipos de destino. El usuario la usa para generar un código de solicitud y después para introducir el código de desbloqueo para activar el acceso temporal una vez que el administrador lo concede. Después de la activación, el usuario tendrá acceso a dispositivos y puertos de conexión (cuando normalmente ese acceso está bloqueado) en su equipo de destino protegido por la duración y el intervalo de tiempo especificados.

I

Informe de resumen

Un informe de resumen que ofrece un reporte de la estadística de actividad detectada por GFI EndPointSecurity.

L

Lista blanca de dispositivos

Una lista de dispositivos específicos cuyo uso está permitido cuando se accede a ellos desde todos los equipos de destino abarcados por la directiva de protección.

Lista negra de dispositivos

Una lista de dispositivos específicos cuyo uso está bloqueado cuando se accede a ellos desde todos los equipos de destino abarcados por la directiva de protección.

M

Mensaje de usuario

Un mensaje que muestran los agentes de GFI EndPointSecurity en los equipos de destino cuando se accede a los dispositivos.

Mensajes de error de implementación

Errores que pueden surgir después de la implementación de agentes de GFI EndPointSecurity desde la consola de administración de GFI EndPointSecurity.

O

Objetos de directiva de grupo

Gestión centralizada de Active Directory y sistema de configuración que controla lo que los usuarios pueden y no pueden hacer en una red informática.

P

Permisos de acceso

Un conjunto de permisos (acceso, lectura y escritura) que se asignan a los usuarios y grupos por categoría de dispositivo, puerto de conectividad o dispositivo específico.

Permisos globales

Un paso del asistente para la creación de directivas de protección que le pide al usuario que bloquee o permita el acceso a todos los dispositivos incluidos en una categoría o que están conectados a un puerto de los equipos de destino abarcados por la directiva de protección.

Puerto de conectividad

Una interfaz entre los equipos y los dispositivos.

R

Registro de eventos

Una función para registrar eventos relacionados con los intentos realizados para acceder a dispositivos y a puertos de conexión en los equipos de destino y operaciones de servicio.

U

Usuario avanzado

Un usuario avanzado obtiene automáticamente acceso total a los dispositivos conectados a cualquier equipo de destino abarcado por la directiva de protección.

17 Índice

U

V

EE.UU., CANADÁ, AMÉRICA CENTRAL Y AMÉRICA DEL SUR

15300 Weston Parkway, Suite 104, Cary, NC 27513, EE.UU.

Teléfono: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

REINO UNIDO Y REPÚBLICA DE IRLANDA

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, REINO UNIDO

Teléfono: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPA, ORIENTE MEDIO Y ÁFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Teléfono: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA Y NUEVA ZELANDA

83 King William Road, Unley 5061, Australia Meridional

Teléfono: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

